Pontifícia Universidade Católica
do Rio de Janeiro

Eduardo José Guedes Magrani

A Internet das Coisas:
Privacidade e Ética na Era da Hiperconectividade

Tese de Doutorado

Tese apresentada como requisito parcial para obtenção do grau de Doutor pelo Programa de Pós-Graduação em Direito do Departamento de Direito na PUC-Rio

Orientadora: Profª. Caitlin Sampaio Mulholland

Rio de Janeiro
Abril de 2018

Pontifícia Universidade Católica
do Rio de Janeiro

Eduardo José Guedes Magrani

A Internet das Coisas:
Privacidade e Ética na Era da Hiperconectividade

Tese apresentada como requisito parcial para obtenção do grau de Doutor pelo Programa de Pós-graduação em Direito da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Profª. Caitlin Sampaio Mulholland
Orientadora
Departamento de Direito – PUC-Rio

Profª. Gisele Guimarães Cittadino
Departamento de Direito – PUC-Rio

Prof. Carlos Affonso Pereira de Souza
Departamento de Direito – PUC-Rio

Prof. Sérgio Vieira Branco Júnior
IBMEC

Prof. Danilo César Maganhoto Doneda
FGV-RJ

Prof. Augusto César Pinheiro da Silva
Vice-Decano Setorial de Pós-Graduação do
Centro de Ciências Sociais - PUC-Rio

Rio de Janeiro, 17 de abril de 2018.

Eduardo José Guedes Magrani

Coordenador do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Senior Fellow na Universidade Humboldt de Berlim. Pesquisador da Law Schools Global League. Doutor e Mestre em Direito Constitucional pela PUC-Rio. Bacharel em Direito pela PUC-Rio, com intercâmbio na Universidade de Coimbra e Université Stendhal-Grenoble. Professor de Direito e Tecnologia e Propriedade Intelectual na FGV, IBMEC e PUC-Rio. Advogado atuante nos campos de Direitos Digitais, Direito Societário e Propriedade Intelectual. Autor de diversos livros e artigos na área de Tecnologia e Propriedade Intelectual, dentre eles os livros: "Democracia Conectada" e "Digital Rights: Latin America and the Caribbean" e "A Internet das Coisas"

Ficha Catalográfica

Magrani, Eduardo José Guedes

A Internet das Coisas: Privacidade e Ética na Era da Hiperconectividade / Eduardo José Guedes Magrani; orientadora: Caitlin Sampaio Mulholland. – Rio de Janeiro: PUC-Rio, Departamento de Direito, 2018

333 f. : 30 cm

Tese (doutorado) – Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Direito.

Inclui Referências bibliográficas

1. Direito - Teses. 2. Internet das Coisas; 3. Tecno-regulação; 4. Web 3.0; 5. Hiperconectividade; 6. Regulação; 7. Inovação; 8. Ética do Discurso; 9. Ética da Informação; 10. Filosofi da Tecnologia; 11. Privacidade; 12. Direitos fundamentais; 13. Estado de Direito. I. Mulholland, Caitlin Sampaio. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Direito. III. Título.

CDD: 340

Agradecimentos

Caitlin Sampaio

Sérgio Branco

Carlos Affonso

Danilo Doneda

Ronaldo Lemos

Luiz Abrahão

Christian Marks e Christian Djeffal

Bartira, Fabio e Sylvio Magrani

Ana Lucia, Cristina, Felipe e Bruno Magrani

Lucy Massa

Júlia Costa

Octavio, Tito e Caio Guedes

Adriana Bittencourt

Ana Lara Mangeth

Gabriella Cantanhede

Pedro Augusto Francisco

Fernando Lennertz

Chiara de Teffé

Luca Belli

Vanessa Tourinho

Renan Medeiros

Helena Ferreira

Luã Fergus

O sábio homem, racional, usuário e engenheiro das coisas, engenhou tanto que a coisa coisificou lógico-racionalmente o homem. O homem-coisa se engendrou em uma labiríntica teia sociotécnica onto-epistemológica *nouveau*. Fica agora o filosofar daquele que já não é. Como diria o poeta Mario Quintana: o mais difícil mesmo é a arte de desler. Sob os feixes tímidos-*vintage* do antropoceno iluminista que ainda nos banha, dedico esta materialidade dialógica à misteriosa força que nos move e à enigmática teia que nos une.

Resumo

Magrani, Eduardo José Guedes; Mulholland, Caitlin Sampaio. **A Internet das Coisas: Privacidade e Ética na Era da Hiperconectividade**. Rio de Janeiro, 2018. 333p Tese de Doutorado - Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro.

A interação contínua entre dispositivos inteligentes, sensores e pessoas aponta para o número crescente de dados que estão sendo produzidos, armazenados e processados, alterando, sob diversos aspectos e de forma crescente, nosso cotidiano. Por um lado, o contexto de hiperconectividade pode trazer benefícios econômicos ao Estado, a empresas, bem como comodidade aos consumidores. Por outro, a crescente conectividade traz desafios significativos nas esferas de proteção da privacidade e à ética contemporânea, impactando, em última instância, a própria democracia. Este trabalho aborda, principalmente sob o ponto de vista regulatório, alguns destes desafios enfrentados pelo atual Estado de direito decorrentes do avanço do cenário denominado de Internet das Coisas.

Palavras-chave

Internet das Coisas; Tecno-regulação; Web 3.0; Hiperconectividade; Regulação; Inovação; Ética do Discurso; Ética da Informação; Filosofia da Tecnologia; Privacidade; Direitos fundamentais; Estado de Direito.

Abstract

Magrani, Eduardo José Guedes; Mulholland, Caitlin Sampaio (Advisor)**. The Internet of Things: Privacy and Ethics in the Age of Hyperconnectivity**. Rio de Janeiro, 2018. 333p. Tese de Doutorado - Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro

The continuous interaction between intelligent devices, sensors and people points to the increasing number of data being produced, stored and processed, changing, in various aspects and increasingly, our daily life. On one hand, the context of hyperconnectivity can bring economic benefits to the State, companies, as well as convenience to consumers. On the other hand, increasing connectivity brings significant challenges in the spheres of privacy protection and contemporary ethics, impacting, ultimately, democracy itself. This thesis addresses, from the regulatory point of view, some of these challenges faced by the current rule of law arising from the advance of the scenario called Internet of Things.

Keywords

Internet of Things; Techno-regulation; Web 3.0; Hyperconnectivity Regulation; Innovation; Discourse Ethics; Information Ethics; Phylosophy of Technology; Privacy; Fundamental rights; Rule of law.

"*Anything that can be connected*, will be connected."
(J. Morgan)

Sumário

Introdução

A tecnologia está mudando rapidamente a maneira como interagimos com o mundo à nossa volta. Visando a atender às mais novas demandas dos consumidores, empresas hoje estão desenvolvendo produtos com interfaces tecnológicas que seriam inimagináveis há uma década.

Sistemas automatizados que acendem as luzes e aquecem o jantar ao perceber que você está retornando do trabalho para casa, pulseiras e palmilhas inteligentes que compartilham com seus amigos o quanto você andou a pé ou de bicicleta durante o dia na cidade ou sensores que avisam automaticamente aos fazendeiros quando um animal está doente ou prenhe.[1] Todos esses exemplos são manifestações consideradas tecnologias inovadoras associadas ao conceito que vem sendo construído de "Internet das Coisas" (*Internet of Things* – doravante, "*IoT*").

Existem fortes divergências em relação ao conceito[2] de IoT, não havendo, portanto, um conceito único que possa ser considerado pacífico ou unânime. De maneira geral, pode ser entendido como um ambiente de objetos físicos interconectados com a Internet, por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado a facilitar o cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia.

Segundo o Consórcio[3] formado por McKinsey & Company, Fundação CPqD e Pereira Neto | Macedo Advogados, responsáveis por desenvolver o Plano

[1] Vide informativo disponível em: <http://www.computersciencezone.org/wp-content/uploads/2015/04/Security-and-the-Internet-of-Things.jpg#sthash.c6u2POMr.dpuf>. Acesso em: 27 mar. 2017.

[2] O pesquisador na área de tecnologia Silvio Meira define as "coisas", no sentido da Internet das Coisas, como dispositivos que possuem, simultaneamente, capacidades de computação, comunicação e controle. Se o dispositivo está no plano da computação e da comunicação, mas não tem sensores ou atuadores que lhe confiram a característica do controle, é [apenas] uma máquina em rede; se não possui capacidade de comunicação, é um sistema de controle digital; se não conta com capacidades computacionais, é um sistema de telemetria. As coisas, na Internet das Coisas, devem ter as três características ao mesmo tempo, todas inseridas no meio digital. Segundo Meira, seria inclusive possível dizer que as "coisas", neste contexto, são *objetos digitais completos*. MEIRA, Silvio. SINAIS do FUTURO IMEDIATO, #1: Internet das coisas. *ikewai*, Recife, dez. 2016. Disponível em: <http://www.ikewai.com/WordPress/2016/12/12/sinais-do-futuro-imediato-1-Internet-das-coisas/>. Acesso em: 27 mar. 2017.

[3] LEMOS, Ronaldo, et al. *O Direito da Internet das Coisas: desafios e perspectivas de IoT no Brasil.* 2018. Disponível em: <https://www.jota.info/artigos/o-direito-da-internet-das-coisas-desafios-e-perspectivas-de-iot-no-brasil-09012018>. Acesso em: 27 mar. 2017.

Nacional de IoT no Brasil, Internet das Coisas é a expressão que busca designar todo um conjunto de novos serviços e dispositivos que reúnem ao menos três pontos elementares: conectividade, uso de sensores/atuadores e capacidade computacional de processamento e armazenamento de dados. Para o consórcio PoETAS.IT (Políticas e Estratégias para Tecnologias, Aplicações e Serviços para a Internet de Tudo)[4], o conceito de IoT consiste em estar tudo interconectado: itens do dia a dia, máquinas e objetos em geral, ligados à rede mundial de computadores e operando em coordenação e sintonia com as TICs (Tecnologias da Informação e Comunicação). Já para Olga Cavalli, "o que hoje é chamado de IoT é um conjunto de tecnologias e protocolos associados que permitem que objetos se conectem a uma rede de comunicações e são identificados e controlados através desta conexão de rede".[5]

O que todas as definições de IoT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam as informações/dados em um contexto de hiperconectividade[6-7].

O termo hiperconectividade foi cunhado inicialmente para descrever o estado de disponibilidade dos indivíduos para se comunicar a qualquer momento. Este termo possui alguns desdobramentos importantes[8]. Podemos citar alguns deles: o conceito de *always-on*, estado em que as pessoas estão conectadas a todo o momento; a possibilidade de estar prontamente acessível (*readily accessible*); a riqueza de informações; a interatividade; e o armazenamento ininterrupto de

[4] FTC Staff Report. *Internet of Things*: privacy & security in a connected world. 2015. 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: 28 mar. 2017.

[5] CAVALLI, Olga. Internet das Coisas e Inovação na América Latina. 2016 (mimeo).

[6] Cf. vídeo explicativo do NIC.br sobre IoT, disponível em: <https://www.youtube.com/watch?v=jlkvzcG1UMk>. Acesso em: 27 mar. 2017.

Para o consórcio PoETAS.IT (Políticas e Estratégias para Tecnologias, Aplicações e Serviços para a Internet de Tudo), o conceito de IoT consiste em estar "Tudo interconectado: itens do dia a dia, máquinas e objetos em geral, ligados à rede mundial de computadores e operando em coordenação e sintonia". Além disso, o conceito se relaciona com o chamado "ABC" (*Analytics* + *Big Data* + *Cloud Computing*) das TICs (Tecnologias da Informação e Comunicação[7]). Disponível em: <http://poetas.it.cesar.org.br/index.php/POETAS.IT:Sobre>. Acesso em: 27 mar. 2017.

[8] Sobre este assunto, veja-se QUAN-HAASE, Anabel; WELLMAN, Barry. Hyperconnected Net Work: Computer-Mediated Community in a High-Tech Organization. In: ADLER, Paul S.; HECKSCHER, Charles. Towards Collaborative Community. p. 285. Disponível em: <http://groups.chass.utoronto.ca/netlab/wp-content/uploads/2012/05/Hyperconnected-Net-Work.pdf>. Acesso em: 27 mar. 2017.

dados (*always recording*)[9]. O termo hiperconectividade encontra-se hoje atrelado às comunicações entre indivíduos (*person-to-person*, P2P), indivíduos e máquina (*human-to-machine*, H2M) e entre máquinas (*machine-to-machine*, M2M) valendo-se, para tanto, de diferentes meios de comunicação[10 - 11]. Há, neste contexto, um fluxo contínuo de informações e massiva produção de dados.

Por isso, o avanço da hiperconexão depende do aumento de dispositivos que enviam e recebem estas informações. Exemplos disto são os inúmeros *wearables* disponíveis no mercado e as várias opções de sensores utilizados no setor agrícola e nas indústrias[12]. Quanto maior o número de dispositivos conectados, mais dados são produzidos[13].

Todos os dias, "coisas" se conectam à Internet com capacidade para compartilhar, processar, armazenar e analisar um volume enorme de dados[14]. Esta

[9] Cf. FREDETTE, John et al. The Promise and Peril of Hyperconnectivity for Organizations and Societies. In: INSEAD & World Economic Forum. *The Global Information Technology Report 2012*: Living in a Hyperconnected World. Genebra, 2012. p. 113. Disponível em: <https://pdfs.semanticscholar.org/68bb/365887b24ba1e541e3e2b8feb4569b94903d.pdf#page=139>. Acesso em: 27 mar. 2017.

[10] Veja-se: BREWSTER, Tom. *When machines take over*: our hyperconnected world. BBC, 25 jan. 2014. Disponível em: <http://www.bbc.com/capital/story/20140124-only-connect>. Acesso em: 27 mar. 2017.

[11] Cf. FREDETTE, John et al. The Promise and Peril of Hyperconnectivity for Organizations and Societies. In: INSEAD & World Economic Forum. *The Global Information Technology Report 2012*: Living in a Hyperconnected World. Genebra, 2012. p. 113. Disponível em: <https://pdfs.semanticscholar.org/68bb/365887b24ba1e541e3e2b8feb4569b94903d.pdf#page=139>. Acesso em: 27 mar. 2017.

[12] Cf. TECHTARGET ANZ STAFF. What is hyperconnectivity? *Computer weekly*, 19 fev. 2007. Disponível em: <http://www.computerweekly.com/news/2240100953/What-is-hyperconnectivity>. Acesso em: 27 mar. 2017.

[13] Não obstante, a hiperconectividade tem ainda como limitação o "mito do acesso". Em outras palavras, enquanto parte da sociedade experimenta os efeitos da hiperconectividade, outra parte sequer possui acesso à Internet e está excluída de todo este processo.

[14] O filósofo italiano Luciano Floridi, pesquisador do Oxford Internet Institute (OII) faz uma distinção relevante entre 'dados' e 'informação'. Segundo Floridi, 'dados' possuem um conceito mais amplo tendo em vista que podem se encontrar em formato não estruturado. Nesse formato não possuem, segundo o Floridi, nenhum tratamento atributivo de valor para que seja considerado uma informação relevante. Portanto, para Floridi, dados somente merecem a valorização como informação após serem tratados, entre outras qualidades (*well-formed, meaningful and truthful data*). Essa diferenciação importa na hora de se avaliar tecnicamente o peso de um dado, genericamente falando, e de uma informação, pelo fato de consubstanciar um elemento de maior valor social e mercadológico. Para os fins deste trabalho, no entanto, trabalharemos com ambos os conceitos de forma indistinta. "*Over the last three decades, several analyses in Information Science, in Information Systems Theory, Methodology, Analysis and Design, in Information (Systems) Management, in Database Design and in Decision Theory have adopted a General Definition of Information (GDI) in terms of data + meaning. GDI has become an operational standard, especially in fields that treat data and information as reified entities (consider, for example, the now common expressions "data mining" and "information management"). Recently, GDI has begun to influence the philosophy of computing and information (Floridi [1999] and Mingers [1997]). A clear way of formulating GDI is as a tripartite defintion: The General*

prática é o que une o conceito de IoT ao conceito de *Big Data*. *Big Data* é um termo em evolução que descreve qualquer quantidade volumosa de dados estruturados, semiestruturados ou não estruturados[15] que têm o potencial de ser explorados para obter informações[16].[17]

A primeira propriedade envolvendo *Big Data* consiste no volume crescente de dados[18]. Pesquisa recente da Cisco[19] estima que, nos próximos anos,

---

Definition of Information (GDI): information, understood as semantic content, if and only if: (GDI.1) σ consists of one or more data; (GDI.2) the data in σ are well-formed; (GDI.3) the well-formed data in σ are meaningful. GDI requires a definition of data. This will be provided in the next section. Before, a brief comment on each clause is in order. According to (GDI.1), data are the stuff of which information is made. We shall see that things can soon get more complicated. In (GDI.2), "well-formed" means that the data are clustered together correctly, according to the rules (syntax) that govern the chosen system, code or language being analysed. Syntax here must be understood broadly (not just linguistically), as what determines the form, construction, composition or structuring of something (engineers, film directors, painters, chess players and gardeners speak of syntax in this broad sense). Disponível em: <https://plato.stanford.edu/entries/information-semantic/.> Acesso em: 27 mar. 2017.

[15] "A informação armazenada nos bancos de dados é conhecida como dados estruturados, porque é representada em um formato estrito. Por exemplo, cada registro em uma tabela de banco de dados relacional. Já os dados não-estruturados são quaisquer documentos, arquivos, gráficos, imagens, textos, relatórios, formulários ou gravações de vídeo ou áudio que não tenha sido codificados, ou de outra forma estruturados em linhas e colunas ou registros. De acordo com muitas estimativas, cerca de 90% de todos os dados armazenados são mantidos fora de bancos de dados relacionais. De todos os dados do mundo que foram gerados nos últimos anos apenas 10% destes dados estão estruturados. Os 90% restantes estão desestruturados e se reúnem na sua grande parte nas redes sociais como Facebook, Twitter, Pinterest, entre outras. O uso do Big Data nas redes sociais tem como objetivo buscar soluções para organizar o grande volume de dados que cresce absurdamente a cada dia na web. Diariamente, uma gigante quantidade de dados é literalmente jogada, armazenada e manipulada". TESSAROLO, Pedro e MAGALHÃES, William. A ERA DO BIG DATA NO CONTEÚDO DIGITAL: OS DADOS ESTRUTURADOS E NÃO ESTRUTURADOS. Disponível em: <http://web.unipar.br/~seinpar/2015/_include/artigos/Pedro_Henrique_Tessarolo.pdf>. Acesso em: 27 mar. 2017.

[16] LANE, Julia (org.). *Privacy, Big Data and the Public Good*: frameworks for engagement. Cambridge University Press. 2014.

[17] "*As information has become a central issue in almost all of the sciences and humanities this development will also impact philosophical reflection in these areas. Archaeologists, linguists, physicists, astronomers all deal with information. The first thing a scientist has to do before he can formulate a theory is gathering information. The application possibilities are abundant. Datamining and the handling of extremely large data sets seems to be an essential for almost every empirical discipline in the 21st century*". Vide: https://plato.stanford.edu/entries/information/.

[18] Cf. RIJMENAM, Mark van. Why the 3 V's are Not Sufficient to Describe Big Data. *DATAFLOQ*, ago. 2015. Disponível em: <https://datafloq.com/read/3vs-sufficient-describe-big-data/166>. Acesso em: 27 mar. 2017.

[19] CISCO. The Zettabyte Era: Trends and Analysis. *Cisco*, jun. 2016. Disponível em <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html>. Acesso em: 27 mar. 2017.

a medida em Gigabytes[20] será superada e o cálculo da quantidade de dados será feito na ordem Zettabyte[21] e até mesmo em Yottabyte[22].

Outra propriedade envolve a alta velocidade[23] com que os dados são produzidos, analisados e visualizados. Além disso, a variedade de formatos de dados representa um desafio adicional. Esta característica é potencializada pelos diferentes dispositivos responsáveis por coletar e produzir dados em diversos âmbitos. As informações produzidas por um mecanismo que monitora a temperatura são bem diferentes das obtidas em redes sociais, por exemplo. Ademais, a maioria dos dados encontrados não é estruturada[24].

O conceito[25] de *Big Data*[26] pode implicar ainda, juntamente com o conceito de *Data Science*[27], na capacidade de transformar dados brutos em

[20] Gigabyte é uma unidade de medida de informação que equivale a 1 000 000 000 bytes.
[21] Zettabyte é uma unidade de informação que corresponde a 1.000.000.000.000.000.000.000 (10^{21}) bytes.
[22] Yottabyte é uma unidade de medida de informação que equivale a 10 elevado a 24 bytes.
[23] Cf. RIJMENAM, Mark van. Why the 3 V's are Not Sufficient to Describe Big Data. *DATAFLOQ*, ago. 2015. Disponível em: <https://datafloq.com/read/3vs-sufficient-describe-big-data/166>. Acesso em: 27 mar. 2017..
[24] RIJMENAM, Mark van. Why the 3 V's are Not Sufficient to Describe Big Data. *DATAFLOQ*, ago. 2015. Disponível em: <https://datafloq.com/read/3vs-sufficient-describe-big-data/166>. Acesso em: 27 mar. 2017. Veja-se, ainda, MOLARO, Cristian. Do not Ignore Structured Data in Big Data Analytics: the important role of structured data when gleaning information from Big Data. *IBM Big Data & Analytics Hub*, 19 jul. 2013. Disponível em: <http://www.ibmbigdatahub.com/blog/do-not-ignore-structured-data-big-data-analytics>. Acesso em: 27 mar. 2017.
[25] Segundo o estudo do ITS Rio de 2016, Global South Project Report on the Brazilian Case Studies: "*Big Data is literally those sets of data, whose existence is possible solely as a consequence of the massive data collection that has become widespread in recent years, thanks to the ubiquitous presence of devices and sensors in everyday life, and the increasing number of people connected to such technologies through digital networks as well of sensors. All actions and communications in digital platforms, such as with mobile phones, computers, or even credit card transactions and, more recently, income tax declarations, or actions that are at some point digitized and thus transformed in data, such as CCTV cameras coupled with facial or pattern recognition software11, are prone to be stored, processed, copied and distributed almost instantaneously, allowing for data analyses that may lead to presumably more well-informed decision making by governments and businesses alike*." In: Big Data in the Global South Project Report on the Brazilian Case Studies. 2016.
[26] Para o professor da Universidade Federal de Pernambuco, José Carlos Cavalcanti, o conceito de Big Data se aplica a informações que não podem ser processadas ou analisadas usando processos ou ferramentas tradicionais. Cavalcanti menciona como características básicas do conceito de Big Data: volume, variedade e velocidade (os chamados 3Vs, que consistem em um conceito previamente criado por outros autores), reconhecendo também a "veracidade" como outra possível característica defendida por outros autores. CAVALCANTI, Jose Carlos. The new ABC of ICTs (Analytics + Big Data + Cloud Computing): a complex trade off between IT and CT costs. In: MARTINS, Jorge Tiago; MOLNAR, Andreea (Orgs.). *Handbook of Research on Innovation in Information Retrieval, analysis and management*. Hershey: IGI Global, 2016. Disponível em: http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-GlobalPulseMay2012.pdf. Acesso em: 28 mar. 2017.

gráficos e tabelas que permitam a compreensão do fenômeno a ser demonstrado. É importante mencionar que, em um contexto em que decisões são tomadas cada vez mais com base em dados, é de extrema importância garantir a veracidade destas informações[28].

Nas palavras de Maike Wile, *Big Data* é mais que um emaranhado de dados, pois é essencialmente relacional. Apesar de isso não ser um fenômeno novo, o que a Internet fez foi dar uma nova dimensão, transformando-o. Para bem entender essas transformações, segundo Wile, precisamos compreender que o *Big Data* somos nós[29].

Segundo Hannes Grassegger e Mikael Krogerus[30]:

> Qualquer pessoa que não tenha passado os últimos cinco anos vivendo em outro planeta estará familiarizado com o termo Big Data. Big Data significa, em essência, que tudo o que fazemos, tanto online como offline, deixa vestígios digitais. Cada compra que fazemos com nossos cartões, cada busca que digitamos no Google, cada movimento que fazemos quando nosso telefone celular está em nosso bolso, cada "like" é armazenado. Especialmente cada "like". Durante muito tempo, não era inteiramente claro o uso que esses dados poderiam ter – exceto, talvez, que poderíamos encontrar anúncios de remédios para hipertensão logo após termos pesquisado no Google "reduzir a pressão arterial.[31]

---

[27] A ciência dos dados é um campo interdisciplinar que envolve métodos, processos e sistemas científicos para extrair conhecimento, valor e insights a partir de dados estruturados ou não estruturados. Portanto, a ciência de dados permite a extração de informações valiosas a partir dos dados. A ciência de dados difere das análises estatísticas e da ciência da computação em seu método aplicado a dados coletados usando princípios científicos. Como estamos vivendo na era do Big Data, a Ciência de dados está se tornando um campo muito promissor para explorar e processar grandes volumes de dados gerados a partir de várias fontes e em diferentes velocidades, produzindo resultados relevantes para indústria e sociedade. Disponível em: https://www.datascienceacademy.com.br/course?courseid=introduo--cincia-de-dados. Acesso em: 28 mar. 2017.

[28] Cf. MCNULTY, Eileen. Understanding Big Data: The Seven V's. *Dataconomy*, 22 mai. 2014. Disponível em: <http://dataconomy.com/2014/05/seven-vs-big-data/>. Acesso em: 27 mar. 2017.

[29] SANTOS, Maike Wile dos. O Big Data somos nós: a humanidade de nossos dados. *Jota*, 16 mar. 2017. Disponível em: <https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-big-data-somos-nos-a-humanidade-de-nossos-dados-16032017>. Acesso em: 27 mar. 2017.

[30] GRASSEGGER, Hannes & KROGERUS, Mikael. The Data That Turned the World Upside Down. *Motherboard*, 28 jan. 2017. Disponível em: <https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win>. Acesso em: 27 mar. 2017.

[31] Tradução livre do autor. No original: "*Anyone who has not spent the last five years living on another planet will be familiar with the term Big Data. Big Data means, in essence, that everything we do, both on and offline, leaves digital traces. Every purchase we make with our cards, every search we type into Google, every movement we make when our mobile phone is in our pocket, every "like" is stored. Especially every "like." For a long time, it was not entirely clear what use this data could have — except, perhaps, that we might find ads for high blood pressure remedies just after we've Googled "reduce blood pressure.*"

A combinação entre objetos inteligentes e *Big Data* poderá alterar significativamente a maneira como vivemos[32]. Algumas pesquisas[33] estimam que em 2020 a quantidade de objetos interconectados passará dos 25 bilhões, podendo chegar a 50 bilhões de dispositivos inteligentes. As projeções para o impacto deste cenário de hiperconexão na economia são impressionantes. A estimativa de impacto econômico global corresponde a mais de US$ 11 trilhões de dólares em 2025[34].

Por conta de estimativas como essas, a IoT vem recebendo fortes investimentos do setor privado e surge como possível solução diante dos novos desafios de gestão pública, prometendo, a partir do uso de tecnologias integradas e do processamento massivo de dados, soluções mais eficazes para problemas como poluição, congestionamentos, criminalidade, eficiência produtiva, entre outros.

Além disso, a IoT poderá trazer inúmeros benefícios aos consumidores. Dispositivos de saúde interconectados permitirão monitoramento mais constante e eficiente e interação mais eficaz entre paciente e médico. Sistemas de automação residencial permitirão que um consumidor, antes mesmo de chegar em casa, possa enviar mensagem para que os próprios dispositivos realizem ações para abrir os portões, desligar alarmes, preparar o banho quente, colocar música ambiente e alterar a temperatura da casa.

Por outro lado, esses inúmeros dispositivos conectados que nos acompanharão diária e constantemente em nossas rotinas, irão coletar, transmitir, armazenar e compartilhar uma quantidade enorme de dados, muitos deles estritamente particulares e mesmo íntimos. Com o aumento exponencial de utilização destes dispositivos que já se encontram ou que entrarão em breve no mercado, devemos estar atentos aos riscos que isso pode trazer para a privacidade e segurança dos usuários.

---

[32] FTC Staff Report. *Internet of Things*: privacy & security in a connected world. 2015. 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: 28 mar. 2017.

[33] Veja-se: BARKER, Colin. 25 billion connected devices by 2020 to build the Internet of Things. *ZDNet*, 11 nov. 2014. Disponível em: <http://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-Internet-of-things/>. Acesso em: 27 mar. 2017.

[34] ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. *The Internet of Things*: An Overview. Understanding the Issues and Challenges of a More Connected World. ISOC, 2015, pp. 1 e 4. Disponível em: <https://www.Internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf>. Acesso em: 30 mar. 2017.

Ademais, toda essa hiperconectividade e interação contínua entre diversos aparelhos, sensores e pessoas, alteraram a forma como agimos comunicativamente e tomamos decisões nas esferas pública e privada. Cada vez mais as informações que circulam pela Internet não serão mais colocadas na rede tão somente por pessoas, mas por Coisas e algoritmos[35] dotados de inteligência artificial[36] que trocam dados e informações entre si, formando um espaço de conexões de rede e informações cada vez mais automatizado.

Observamos hoje a construção de novas relações que estamos estabelecendo com as máquinas e demais dispositivos interconectados permitindo que algoritmos passem a tomar decisões e a pautar avaliações e ações que antes eram tomadas por humanos. Essa ainda é uma cultura relativamente recente e implica em considerações éticas importantes tendo em vista os impactos cada vez maiores da comunicação algorítmica na sociedade.

Levando em consideração o quão recente é esse cenário digital de hiperconectividade e de IoT baseado na relação estreita entre objetos inteligentes,

[35] Entendemos neste trabalho o termo "algoritmos" como conjuntos de regras que os computadores seguem para resolver problemas e tomar decisões sobre um determinado curso de ação. Em termos mais técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa, ou seja, uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa.

[36] A inteligência artificial ("IA" ou *Artificial Intelligence* - "AI") é um sub-campo da informática. Seu objetivo é habilitar o desenvolvimento de computadores que sejam capazes de fazer coisas normalmente realizadas por pessoas - em particular, coisas associadas a pessoas que atuam de forma inteligente. O pesquisador de Stanford, John McCarthy, cunhou o termo em 1956 (durante a Conferência de Dartmouth). Com esta definição, qualquer programa poderia ser considerado AI se for capaz de fazer algo que normalmente pensamos ser inteligente em seres humanos. A forma como se realiza a tarefa não é o problema segundo esta concepção, importa apenas ser capaz de fazê-la. Outros simplesmente requerem que o trabalho seja realizado e não se importam se o cálculo tiver algo a ver com o pensamento humano. Outras concepções estão no meio, usando o raciocínio humano como modelo que pode informar e inspirar, mas não restritos à ideia de imitação dos humanos. O trabalho destinado a simular verdadeiramente o raciocínio humano tende a ser chamado de "AI forte", na medida em que qualquer resultado pode ser usado não só para construir sistemas que pensam, mas também para explicar como os humanos pensam. Há outra distinção a ser feita - a diferença entre os sistemas de AI projetados para tarefas específicas (geralmente denominados "IA limitados") e os poucos sistemas que são projetados para a capacidade de raciocinar em geral (referido como "AI geral")". O conceito de inteligência artificial, de maneira geral, vem sendo alvo de críticas por conduzir a problemas semânticos. A ideia da artificialidade, para a parte majoritária dos teóricos, está ligada ao ímpeto de emularmos tecnicamente a inteligência humana em agentes não-humanos. No entanto, ainda que seja uma meta ambiciosa, a inteligência artificial já demonstra um avanço enorme em relação à sua capacidade lógico-racional, fazendo com que a emulação da inteligência lógico-racional humana seja algo superável nos próximos anos. O conceito, portanto, tende a ficar defasado, tornando-se limitador em sua própria semântica. Por conta da indeterminação deste termo, alguns teóricos optam por substituir a expressão por "Inteligência Computacional", entre outras nomenclaturas. Disponível em: https://www.computerworld.com/article/2906336/emerging-technology/what-is-artificial-intelligence.html. Acesso em: 28 mar. 2017.

Big Data e Inteligência Computacional[37] ou ainda, entre o chamado "ABC"[38] das Tecnologias da Informação e Comunicação – *Analytics* + *Big Data* + *Cloud Computing* [39] – [40], ainda não temos consciência plena dos seus potenciais benefícios e riscos. Devemos buscar, no entanto, o balanço adequado na regulação[41] jurídica de forma a não engessar a inovação, mas garantindo que o Direito avance também nesta seara, buscando normas apropriadas às novas tecnologias e ao cenário de IoT.

Recentemente, testemunhamos o primeiro acidente fatal envolvendo um piloto automático de carro (da empresa Tesla)[42]. Presenciamos, ainda, o carro

[37] Comumente chamada de Inteligência Artificial (I.A.).

[38] CAVALCANTI, Jose Carlos. The new ABC of ICTs (Analytics + Big Data + Cloud Computing): a complex trade off between IT and CT costs. In: MARTINS, Jorge Tiago; MOLNAR, Andreea (Orgs.). *Handbook of Research on Innovation in Information Retrieval, analysis and management*. Hershey: IGI Global, 2016.

[39] O termo *cloud computing* (ou nuvem, em português) consiste no ambiente criado dentro da Internet principalmente para armazenamento de todo tipo de informação, incluindo fotos, músicas, documentos e vídeos. Dessa forma, os dados ficam guardados em servidores remotos, permitindo o acesso fácil e rápido de qualquer dispositivo conectado à internet.

[40] "Podem ser entendidas como um conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e comunicação dos processos de negócios, da pesquisa científica e de ensino e aprendizagem." Vide: TOTLAB. O que é TIC? *TotLab*, mai 2012. Disponível em: <http://totlab.com.br/noticias/o-que-e-tic-tecnologias-da-informacao-e-comunicacao/>. Acesso em: 31 mar. 2017.

[41] Alguns doutrinadores, fazem uma diferenciação conceitual entre os termos "regulação" e "regulamentação", que será seguida ao longo deste trabalho. "Regulamentação: Formado de *regulamentar (*expedir regulamento, prescrever regras sobre forma), designa a instituição de normas ou de regras referentes ao funcionamento de certas coisas e à excução de atos. Ou a disposição de forma para que se apliquem ou se cumpram medidas ou regras legais. A *regulamentação*, pois, importa na disposição ou na ordenação de *regras suplementares* ou *subsidiárias*, instituidoras, praticamente, do modo de se conduzirem as coisas, *já reguladas por leis.* Assim, *a regulamentação,* sem se afastar da lei, vem estabelecer a forma ou a conduta de aptidão da mesma lei. Não é pois, de sua função instituir *regra nova*, de caráter substancial, nem estabelecer princípio ou regra, divergente da lei *regulamentada.* O objeto da regulamentação é o de instituir ou de estabelecer *regras práticas ou a prática* para a execução da norma legal. É de sua finalidade, ainda, instituir regras de caráter administrativo ou de gestão, fundadas nas regras ou normas gerais. Em qualquer circunstância, no entanto, a regulamentação restringe-se ao estabelecimento de regras e condições indispensáveis à execução das leis e para que tornem mais efetivas as suas determinações. E, assim, não podem *regularmentamente* ser estabelecidas regras gerais de Direito, nem normas gerais criadoras de Direito, desde que esta é função precípua da lei, objeto da *regulação.* Daí se infere a distinção entre *regular* e *regulamentar,* entre *regulação* e *regulamentação. Regular* é estabelecer a regra geral, a norma jurídica fundamental. É instituir o princípio geral ou dispor a respeito dos direitos fundamentais. Regulamentar é prescrever a forma por que se cumpre a execução das regras jurídicas fundamentais ou das disposições legais, sem ofensa aos preceitos, que tenham implantado. É portanto, *instituir* sobre a execução da lei, tomando as providências indispensáveis a essa execução, ou instituir regras para a execução ou funcionamento de serviços." De Plácido e Silva. VOCABULÁRIO JURÍDICO.Editora Forense.28ª edição. 2010.

[42] Disponível em: http://g1.globo.com/carros/noticia/2016/06/acidente-com-carro-da-tesla-em-modo-semiautonomo-deixa-1-morto.html. Acesso em: 28 mar. 2017.

autônomo do Uber ultrapassar o sinal vermelho em São Francisco[43] e em 2018 atropelando e matando uma mulher nos EUA[44]; o aplicativo de fotos do Google identificar algoritmicamente imagens de pessoas negras como gorilas[45]; o algoritmo de reconhecimento facial do Registro de Motores de Massachusetts equivocadamente etiquetar alguém como um criminoso e revogar sua carteira de motorista[46]; o perfil robótico Tay, da empresa Microsoft, criado para interagir com técnica de *machine learning*[47] no Twitter que virou um bot de ofensas racistas e propagador de discurso de ódio em menos de 24 horas[48] e; a Arábia Saudita como o primeiro país do mundo a conceder cidadania a um robô[49], Sophia, uma máquina dotada de inteligência artificial (que ficou famosa no mundo com um vídeo[50] no qual dizia que destruiria a humanidade), causando polêmica pelo fato de possuir mais direitos do que as mulheres de carne e osso do país.[51]

[43] Disponível em: https://www.dn.pt/sociedade/interior/carro-autonomo-da-uber-filmado-a-passar-um-sinal-vermelho-5554491.html. Acesso em: 28 mar. 2017.

[44] Disponível em: https://g1.globo.com/carros/noticia/carro-autonomo-da-uber-atropela-e-mata-mulher-nos-eua.ghtml?utm_source=facebook&utm_medium=social&utm_campaign=g1. Acesso em: 28 mar. 2017.

45 Disponível em: https://www.terra.com.br/noticias/tecnologia/google-fotos-identifica-pessoas-negras-como-gorilas,1fc48c2b7559103e43ef44dcdc16787el2t0RCRD.html. Acesso em: 28 mar. 2017.

[46] Disponível em: https://www.wired.com/2014/11/algorithms-great-can-also-ruin-lives/. Acesso em: 27 mar. 2017.

[47] *"Machine learning is any methodology and set of techniques that can employ data to come up with novel patterns and knowledge, and generate models that can be used for effective predictions about the data. Machine learning is defined by the capacity to define or modify decision-making rules autonomously"*. OTTERLO, Van. A machine learning view on profiling. In: Hildebrandt M and de Vries K (eds) Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology. Abingdon: Routledge, pp. 41–64.

[48] Disponível em: http://revistagalileu.globo.com/blogs/buzz/noticia/2016/03/microsoft-criou-uma-robo-que-interage-nas-redes-sociais-e-ela-virou-nazista.html. Acesso em: 28 mar. 2017.

[49] O termo "Robô" advem da palavra checa *robota,* que significa servo ou trabalhador forçado. Portanto, na gênese do termo há uma forte vinculação da ideia de robô como um escravo moderno da humanidade. Apesar da robô Sophia chamar atenção pelas suas feições humanísticas, trataremos do conceito de robô neste trabalho englobando tanto os robôs com existência física quanto os imateriais, como algoritmos. Aqui nos importa mais o conteúdo e poder de agência / influência, do que a forma de manifestação autônoma de vontade. Nas palavras de Marco Aurélio Castro: "Atualmente, a geração de robôs vem evoluindo de forma acelerada, produzindo equipamentos semelhantes aos humanos e capazes de ver, ler, falar, aprender e até expressar emoções." Extrai-se daí a complexidade de se regular juridicamente as novas Coisas inteligentes, capazes de imitar o comportamento de outras máquinas, aprender com os próprios erros, demonstrar curiosidade, possuindo alto poder de investigação e processamento ao redor do seu ambiente, além de serem tao criativos e determinados quanto os humanos na busca dos seu propósitos. CASTRO, Marco Aurélio. *Personalidade jurídica do robô e sua efetividade*. Salvador: 2009.

[50] Disponível em: https://www.youtube.com/watch?v=W0_DPi0PmF0. Acesso em: 28 mar. 2017.

[51] Disponível em: https://www.nexojornal.com.br/expresso/2017/10/26/Uma-rob%C3%B4-ganhou-cidadania-na-Ar%C3%A1bia-Saudita.-Qual-o-debate-sobre-o-assunto. Acesso em: 28 mar. 2017.

Diante desse cenário e na carência de regulação adequada pelo Direito, estamos vivenciando uma autoregulação do próprio mercado e uma regulação realizada muitas vezes através do design da tecnologia, o que vem se denominando de "tecno-regulação"[52]. A IoT está avançando mais rápido do que nossa habilidade de garantir a tutela[53] dos direitos individuais e coletivos.

Diante do contexto de constante e intenso armazenamento, tratamento, compartilhamento e monetização dos dados que trafegam online é crucial debatermos as noções de privacidade e ética que deverão nortear os avanços tecnológicos, refletindo sobre o mundo em que queremos viver e em como nos enxergamos nesse mundo de dados e máquinas relacionado ao novo cenário de IoT.

Para tanto, iremos nos debruçar no primeiro capítulo deste trabalho sobre o conceito de tecnologia e inovação, buscando o correto enquadramento das funcionalidades de IoT neste contexto. Em seguida, trataremos da origem e construção do termo IoT explicitando sua relação com as características próprias da Web 3.0 em contraposição às fases anteriores da Web.

Analisaremos, em seguida, o estado da arte da IoT no Brasil no tocante ao seu potencial econômico e social e concluiremos o primeiro capítulo alertando para os riscos existentes à privacidade e à segurança dos usuários demandando uma resposta regulatória do Estado de Direito ao avanço tecnológico, com intuito de proteger os direitos fundamentais.

No segundo capítulo deste trabalho trataremos especificamente dos aspectos regulatórios da IoT no Brasil com relação à proteção da privacidade e dos dados pessoais[54], mapeando as regulamentações vigentes aplicáveis no Brasil

[52] Termo cunhado pelo jus-filósofo italiano Ugo Pagallo.

[53] É preciso que o Direito se ajuste buscando normas adequadas às novas tecnologias e ao cenário de IoT, impedindo uma conjuntura em que a tecno-regulação sobrepõe a regulação pelo direito induzindo nosso comportamento de maneira intransponível e violando potencialmente diversos direitos fundamentais.

[54] Apesar de serem interrelacionados, o conceito de privacidade não se confunde com o conceito de dados pessoais. Para as finalidades deste trabalho partiremos do conceito de privacidade defendido pelo jus-filósofo italiano Stefano Rodotá, como sendo: "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" e defenderemos a tese da proteção da privacidade na era da hiperconectividade como um "direito ao não-rastreio". Com relação ao conceito de proteção de dados pessoais, utilizaremos o enquadramento teórico de Danilo Doneda que define a proteção de dados pessoais como uma garantia de caráter instrumental, derivada da tutela da privacidade, mas que não se limita por esta, fazendo referência a todo leque de garantias fundamentais que se encontram no ordenamento brasileiro. Vide: RODOTÁ, Stefano. (2008). A vida na sociedade de vigilância: a privacidade

e as principais propostas legislativas. Faremos, ainda, o contraste entre as propostas legislativas e a regulação europeia em virtude do maior alinhamento com o ordenamento jurídico brasileiro, em comparação com o sistema norte-americano, e por ter servido de inspiração para a criação dos marcos regulatórios nacionais de proteção da privacidade. Concluiremos este capítulo formulando uma melhor adequação do conceito de privacidade adequada à IoT e sugerindo novas possibilidades tecnológicas de auto-gerenciamento dos dados pessoais como ferramentas complementares à regulação legislativa.

No capítulo terceiro, discutiremos as vertentes e perspectivas éticas que devem nortear o avanço deste novo mundo de dados fortemente relacionado aos conceitos de IoT e de Inteligência Artificial. Sem uma reflexão ética que norteie adequadamente a regulação jurídica, inclusive com relação à tutela da privacidade e dos dados pessoais, essa corre o risco de ser inócua ou nociva à coletividade.

É necessário, portanto, que o avanço jurídico-regulatório a respeito de IoT seja acompanhado de perto por um debate ético maduro e inclusivo na esfera pública brasileira. Defenderemos então a tese de que a intensificação da interação homem-máquina e de decisões algorítmicas no contexto de IoT exigem novas lentes ontológicas e epistemológicas capazes de compreender melhor a influência desses elementos na esfera pública conectada, além da necessidade de uma eficaz governança de dados.

Assim, a maneira como nos relacionamos com as Coisas[55] tende a ser cada vez mais intensa. A governança dos dados e a compreensão e regulação da agência dos actantes[56] humanos e não-humanos neste cenário hiperconectado é fundamental. Benefícios e riscos para empresas, Estado e consumidores devem ser sopesados de forma cautelosa. O direito deve estar atento ao seu papel nesse contexto para, de um lado, não obstaculizar demasiadamente o desenvolvimento econômico e tecnológico em andamento, e, por outro lado, regular com eficácia as

---

hoje. Rio de Janeiro, Renovar. DONEDA, Danilo. (2006). Da privacidade à proteção de dados pessoais. Rio de Janeiro, Renovar.

[55] Compreendendo, neste conceito, os artefatos não-humanos desde máquinas e objetos físicos até algoritmos.

[56] No sentido atribuído pelo antropólogo francês Bruno Latour, o termo "*actantes*" engloba todos os agentes humanos e não-humanos, tendo em vista que o termo "ator" remete usualmente a agentes humanos.

práticas tecnológicas, visando coibir abusos e protegendo os direitos constitucionais vigentes. Exploraremos todas essas questões a partir de agora.

1
Tecnologia, inovação e internet das coisas (“IOT”)

“Buy it, use it, break it, fix it,
Trash it, change it, mail - upgrade it,
Charge it, point it, zoom it, press it,
Snap it, work it, quick - erase it,
Write it, cut it, paste it, save it,
Load it, check it, quit - rewrite it,
Plug it, play it, burn it, rip it,
Drag and drop it, zip - unzip it,
Lock it, fill it, call it, find it,
View it, code it, jam - unlock it,
Surf it, scroll it, pause it, click it,
Cross it, crack it, switch - update it,
Name it, read it, tune it, print it,
Scan it, send it, fax - rename it,
Touch it, bring it, pay it, watch it,
Turn it, leave it, start - format it.
Technologic”
(***Daft Punk***)

A dupla francesa de música eletrônica Daft Punk, formada na década de 1990, tem como fio condutor em suas composições musicais tratar dos efeitos da fusão cada dia mais presente entre homem e máquina. Sua canção “Technologic” (Tecnológico), lançada em 2005, é construída a partir de diversos comandos imperativos relacionados a atividades tecnológicas.

A composição nos leva a refletir sobre como esses termos foram modificados e realocados para o contexto de tecnologia e inovação e, ainda, sobre como estes comandos, considerando o advento relativamente recente da era digital, já estão completamente introjetados em nossa rotina e hábitos digitais diários.

As palavras *tecnologia* e *inovação* são, hoje, correntes e intimamente relacionadas aos ambientes digitais. Observamos isso ao analisar a forma e os espaços nos quais esses termos surgem tanto na imprensa quanto na linguagem

usual.[57] Por exemplo, muitos jornais e revistas têm seções de tecnologia, especificamente para tratar dos assuntos relacionados ao mundo digital e, especialmente, à Internet, com um forte vínculo com o conceito de inovação.[58]

O uso corrente desses dois termos está voltado para as tecnologias de informação e comunicação consideradas como "alta tecnologia" ou "tecnologia de ponta", espelhando as tecnologias mais avançadas atreladas à ideia de "inovação". Também está ligada a essa percepção, além dos exemplos da utilização dos computadores e da Internet, a utilização de energia nuclear, nanotecnologia, biotecnologia, etc.[59]

É importante, no entanto, ter em mente que o significado e a etimologia dessas duas palavras remontam a uma concepção bem mais ampla do que a forma como são tratadas hoje pela imprensa e usualmente pelas pessoas, deslocada de sua construção histórico-cultural.

Além disso, técnica é algo anterior à tecnologia e consiste em um conjunto de conhecimentos e habilidades eficazes desenvolvidos pelo homem para melhorar sua forma de viver.[60] Com o desenvolvimento da sociedade ocidental, à dimensão prática da técnica adicionaram-se as dimensões teórica e científica. Os produtos obtidos a partir das atividades deixaram de ser a preocupação central, cedendo lugar à estrutura organizacional ligada aos fluxos de informação. Assim, surgiu a noção de tecnologia, que não é apenas o estudo de uma arte, mas é um estudo científico, com uma metodologia própria e uma teoria que a embasa.

---

[57] Cf. e.g. REDAÇÃO OLHAR DIGITAL. 5 apostas para 2017 nos principais setores da tecnologia. *Olhar Digital*, 2 jan. 2017. Disponível em: <http://olhardigital.uol.com.br/noticia/5-apostas-para-2017-nos-principais-setores-da-tecnologia/65013>. Acesso em: 27 mar. 2017; VEJA COMO a tecnologia pode deixar a sua casa mais segura. *Olhar Digital*, 2 jan. 2017. Disponível em: <http://olhardigital.uol.com.br/lu-explica/noticia/veja-como-a-tecnologia-pode-deixar-a-sua-casa-mais-segura/64971>. Acesso em: 27 mar. 2017; EM 2016 advogados recorreram à tecnologia para espantar a crise. *Terra Notícias*, 3 jan. 2017. Disponível em: <https://noticias.terra.com.br/dino/em-2016-advogados-recorreram-a-tecnologia-para-espantar-a-crise,2cbd6a01657d0cf1c6c60003480d6bf31euayidm.html>. Acesso em: 27 mar. 2017; REDAÇÃO ADNEWS. Samsung usa tecnologia para ajudar pessoas a superarem medos. *Exame*, 2 jan. 2017. Disponível em: <http://exame.abril.com.br/marketing/samsung-usa-tecnologia-para-superar-medos/>. Acesso em: 27 mar. 2017.

[58] Cf., a título de exemplo, os seguintes *websites*: <www.nytimes.com/pages/technology/index.html>; <www.bbc.com/news/technology>; <www.reuters.com/news/technology>; <www1.folha.uol.com.br/tec> Acesso em: 27 mar. 2017.

[59] Nesse sentido, cf. a página <www.significados.com.br/tecnologia-2/>. Acesso em: 27 mar. 2017.

[60] AGAZZI, Evandro. El impacto epistemológico de la tecnología. *Argumentos*, [s.d.]. Disponível em: <www.argumentos.us.es/numero1/agazzi.htm>. Acesso em: 31 mar. 2017.

A palavra *tecnologia* deriva dos vocábulos gregos *tekhné* (arte,[61] indústria, habilidade) e *logos* (argumento, discussão, razão).[62] A tecnologia, em sua etimologia, consiste, portanto, no conjunto de conhecimentos/saberes, argumentos e razões em torno de uma arte/ofício, ou de um fazer determinado[63]. De outra forma, pode ser entendida como o conjunto dos instrumentos, métodos e técnicas

[61] Para José Ferrater Mora, "'arte' significa certa virtude ou habilidade para fazer ou produzir algo. Fala-se de arte mecânica e de arte liberal. Fala-se igualmente de bela arte e de belas artes (caso em que 'arte' é tomada, em sentido estético, como '*a*' Arte). Esses significados não são totalmente independentes; vincula-os entre si a idéia de fazer – e especialmente de produzir – algo de acordo com certos métodos ou certos modelos (métodos e modelos que podem, por seu turno, descobrir-se mediante arte). Essa multiplicidade e essa unicidade de significado simultâneas apareceram já na Grécia com o termo τέχνη (usualmente traduzido por 'arte') e persistiram no vocábulo latino *ars*.
O termo τέχνη significou 'arte' (em particular 'arte manual'), 'indústria', 'ofício'. Dessa maneira, dizia-se de alguém que 'sabia sua arte' – seu 'ofício' – por ter uma habilidade particular e notória. (...) [P]ode-se concluir que τέχνη designava um 'modo de fazer [incluindo no fazer o pensar] algo'. Enquanto esse 'modo', ela implicava a idéia de um método ou conjunto de regras, havendo tantas artes quanto tipos de objetos ou de atividades e organizando-se tais artes de modo hierárquico, desde a arte manual ou ofício até a suprema arte intelectual do pensar para alcançar a verdade (e, de passagem, reger a sociedade segundo essa verdade). (...) A arte distingue-se dos outros quatro [ciência, saber prático, filosofia e razão] na medida em que é 'um estado de capacidade para fazer algo', sempre que implique um curso verdadeiro de raciocínio, isto é, um método. A arte trata de algo que chega a ser. A arte não trata do que é necessário ou do que não pode ser distinto de como é. Tampouco trata da ação; mas apenas da 'produção' (...) Pode-se continuar falando de arte mecânica ou manual, de arte médica, de arte arquitetônica etc. De certa maneira, além disso, o que hoje chamamos de artes (enquanto belas artes) tem um componente manual que os gregos costumavam enfatizar. (...) Na Idade Média, usou-se o termo *ars* na expressão *artes liberais* (ver TRIVIUM, QUADRIVIUM) num sentido equivalente a 'saber'. As artes liberais distinguiam-se das servis, que eram as artes manuais. Estas incluíam muito do que se denominou 'belas artes', como a arquitetura e a pintura. As belas artes eram principalmente uma questão de ofício, não havendo praticamente distinção entre belas artes e artesanato.
A distinção entre as duas últimas acentuou-se na época moderna e culminou no Romantismo, com a exaltação da 'Arte'. Ainda hoje, muitos estetas e filósofos da arte falam dela como designando apenas as 'belas artes', excluindo o artesanato, ou considerando-o uma arte 'inferior' e subordinada. Em contrapartida, no decorrer do século XX, com as numerosas revoluções artísticas e a uptura da rígida divis"ao entre as diversas belas artes, esvaneceu-se a distinção entre arte e artesanato. A rigor, tornou-se problemática a divisão entre 'arte' e 'não-arte'; a chamada 'arte conceitual', entre outras, mostra isso'" (MORA, José Ferrater. *Dicionario de Filosofia*, tomo I (A-D). 2. ed. ver., aum. e atual. por Josep-Maria Terricabras. São Paulo: Edições Loyola, 2004, p. 199-200).

[62] VERASZTO, Estéfano Vizconde et al. Tecnologia: buscando uma definição para o conceito. *Prisma.com*, n. 7, p. 60-85, 2008. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/viewFile/681/pdf>. Acesso em: 2 maio 2017.

[63] "A distinção entre técnica e arte é escassa quando o que hoje chamamos 'técnica' está pouco desenvolvida. Os gregos usavam o termo τέχνη (freqüentemente traduzido por *ars*, 'arte', e que é raiz etimológica de 'técnica'), para designar uma habilidade mediante a qual se faz algo (geralmente, transforma-se uma realidade natural em uma realidade 'artificial'). A *techné* não é, contudo, uma habilidade qualquer, porque segue certas regras. Por isso *techné* significa também 'ofício'. Em geral, *techné* é toda série de regras por meio das quais se consegue algo" (MORA, José Ferrater. *Dicionario de Filosofia*, tomo I (A-D). 2. ed. ver., aum. e atual. por Josep-Maria Terricabras. São Paulo: Edições Loyola, 2004, p. 2820)

que permitem o aproveitamento prático do conhecimento, voltado para as necessidades humanas.[64]

Segundo Estéfano Vizconde (et al.) em pesquisa sobre o conceito de tecnologia, "na técnica, a questão principal é do como transformar, como modificar. O significado original do termo techné tem sua origem a partir de uma das variáveis de um verbo que significa fabricar, produzir, construir, dar à luz, o verbo teuchô ou tictein, cujo sentido vem de Homero; e teuchos significa ferramenta, instrumento. A palavra tecnologia provém de uma junção do termo tecno, do grego techné, que é saber fazer, e logia, do grego logus, razão. Portanto, tecnologia significa a razão do saber fazer. Em outras palavras o estudo da técnica. O estudo da própria atividade do modificar, do transformar, do agir". [65]

Dentro desse conceito mais amplo, é possível enquadrar como avanços de técnica, que permitiram o desenvolvimento de métodos tecnológicos, por exemplo, a transformação feita pelos povos primitivos de pedras em lâminas para cortar a madeira e caçar animais. Segundo Lucas Karasinki "os primeiros indícios de ferramentas criadas com pedra identificados na Etiópia seriam um marco, algo que data de mais de 2,5 milhões de anos. Com isso, ferramentas básicas, criadas com materiais extremamente rústicos, representam o que seria o período inicial do estudo da técnica."[66]

Em complemento, Estéfano Vizconde, et al. ilustram bem este momento da evolução da técnica fazendo referência também à ficção:[67]

> No filme 2001, Uma Odisséia no Espaço, onde de forma poética-visual, Kubrick (1968)1 reconfigurou os primórdios da humanidade mostrando uma descoberta colossal: a concepção da primeira ferramenta, a criação do primeiro utensílio. O hominídeo ao encontrar um esqueleto de um grande herbívoro, apodera-se de um dos seus maiores ossos e começa a desferir golpes contra os restos esqueléticos. De maneira conjunta, intelecto e instrumento, técnica e pensamento. Este nosso antepassado, ilustrado no filme, associa em seus pensamentos o esqueleto encontrado com o animal real. Aquele osso nunca mais seria apenas um osso. Seria um poderoso instrumento de caça e de defesa. Continuando com a

[64] Nessa linha, cf. CONCEITO de tecnologia. *Conceito.de*, ago. 2015. Disponível em: <http://conceito.de/tecnologia#ixzz4YfibhpPs>. Acesso em: 27 mar. 2017.
[65] VERASZTO, Estéfano Vizconde et al. Tecnologia: buscando uma definição para o conceito. *Prisma.com*, n. 7, p. 60-85, 2008. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/viewFile/681/pdf>. Acesso em: 2 maio 2017.
[66] KARASINSKI, Lucas. O que é tecnologia? *Tecmundo*, 29 jul. 2013. Disponível em: <www.tecmundo.com.br/tecnologia/42523-o-que-e-tecnologia-.htm>. Acesso em: 27 mar. 2017.
[67] VERASZTO, Estéfano Vizconde et al. 2008, Op.cit.

> recordação do filme em um instante de deslumbramento atira o hominídeo atira o osso para cima. Aqui novamente o gênio de Kubrick entrou em ação: o osso girando no céu transformava-se em uma espaçonave que ganhava os confins do universo. Estava iniciada a odisséia do homem rumo ao progresso e ao desenvolvimento científico e tecnológico. (...) Com estas três grandes concepções – a pedra lascada, o fogo e a linguagem – a espécie humana dava um salto muito grande rumo às grandes invenções e às colossais descobertas que acabariam fazendo parte da história da sociedade tal qual a conhecemos em nossos dias. (...) Precisamos lembrar que a nossa história tecnológica começou junto com o primeiro homem quando ele descobriu que era possível modificar a natureza para melhorar as condições de vida de seu grupo. O homem, ao descobrir que poderia modificar o osso, estabelecendo um novo uso para o mesmo, dava o passo inicial para a conquista do átomo e do espaço.

Com o passar do tempo, a ideia de tecnologia foi ganhando novos contornos e especificações e envolve, atualmente, uma extensa rede de pesquisadores e projetos interdisciplinares. O presente estudo não pretende esgotar as discussões que cercam o conceito, mas demonstrar os aspectos principais a ele ligados. Tendo isso em vista, destacamos que a noção de tecnologia é ampla e pode ser tratada por diferentes perspectivas. Nesse sentido, há, por exemplo, estudos sobre a tecnologia da informação[68] e sobre a tecnologia genética e segurança alimentar.[69]

O termo *tecnologia* passou a ter grande importância ao longo e após o período iluminista, bem como no bojo da Revolução Industrial, sendo construído ao longo dos séculos XVIII a XX.[70] Aprofunda-se, nesse período, sua conotação mercadológica e de aplicabilidade industrial, relacionada à capacidade de satisfazer as necessidades humanas por meio de inovações tecnológicas. Nesse período, o desenvolvimento tecnológico esteve ligado à evolução técnica em diversas áreas, como a geração de energia, transportes, comunicações, engenharias mecânica e química e agricultura.[71]

A palavra *inovação*, por sua vez, tem origem latina e deriva do termo *innovatio*, que remete a algo novo, recente. De acordo com o dicionário *Michaelis*, tem o seguinte significado: "1. Ato ou efeito de inovar. 2. Tudo que é

[68] Ver, por exemplo, PINOCHET, Luis Herman Contreras. *Tecnologia da informação e comunicação*. Rio de Janeiro: Elsevier, 2014.
[69] Ver, por exemplo, NORER, Roland (Ed.). *Genetic technology and food safety*. Nova York: Springer, 2016.
[70] BUCHANAN, Robert Angus. History of technology. *Encyclopædia Britannica*, 27 fev. 2017. Disponível em: <https://global.britannica.com/technology/history-of-technology/The-Industrial-Revolution-1750-1900>. Acesso em: 2 maio 2017.
[71] Ibid.

novidade; coisa nova; 3. Introdução de palavra, elemento ou construção nova em uma língua inexistente ou na língua-mãe".[72]

No entanto, explicitar simplesmente o significado de *inovação* não aparenta ser suficiente para denotar uma das suas principais características, qual seja, o impacto econômico do termo. Existe um amplo debate na economia sobre o papel da inovação no processo capitalista. Joseph Schumpeter foi um dos primeiros autores a elevar a inovação a um patamar essencial para a dinamicidade do sistema econômico. Para o autor, "uma inovação, no sentido econômico, somente é completa quando há uma transação comercial envolvendo uma invenção e assim gerando riqueza".[73]

Os neoschumpeterianos[74] aprofundaram o papel que a inovação exerce sobre o sistema econômico e problematizaram sua relação com o conceito de tecnologia. Autores como Christopher Freeman dividiram a inovação em quatro processos diferenciados: incremental, radical, mudanças do sistema tecnológico e mudanças no paradigma técnico-econômico. Para Freeman, uma inovação não necessariamente deve ser tecnológica. Qualquer processo que culmine na criação de um produto ou no oferecimento de um serviço, ou mesmo a forma em que um produto ou serviço é oferecido, é considerado uma inovação.[75]

Tal posição, no entanto, não é pacífica, tendo em vista que o próprio Schumpeter observava a inovação a partir de um ponto de vista estritamente tecnológico. Alguns neoschumpeterianos corroboram com a posição de Schumpeter, tal como Matesco, que acredita que a inovação tecnológica é um elemento essencial para averiguar o desenvolvimento de um país.[76]

---

[72] Disponível em: <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=inova%C3%A7%C3%A3o>. Acesso em: 27 mar. 2017.

[73] SCHUMPETER, J. A. A teoria do desenvolvimento econômico. São Paulo: Nova Cultural, 1988 apud SANTOS, Adriana B. A. dos; FAZION Cíntia B.; MEROE, Giuliano P. S. de. Inovação: um estudo sobre a evolução do conceito de Schumpeter. *Revista Caderno de Administração da Faculdade de Administração da FEA PUC-SP*, São Paulo, v. 5, n. 1, p. 2, 2011. Disponível em: <http://revistas.pucsp.br/index.php/caadm/article/view/9014>. Acesso em: 27 mar. 2017.

[74] Como, por exemplo, Christopher Freeman, Carlota Perez, Richard Nelson, Sidney Winter, Giovani Dosi e Jan Fagerberg.

[75] FREEMAN, Christopher. *Technology, policy, and economic performance*: lessons from Japan. Great Britain: Pinter Publishers, 1989 apud SANTOS, Adriana B. A. dos; FAZION Cíntia B.; MEROE, Giuliano P. S. de. "Inovação: um estudo sobre a evolução do conceito de Schumpeter", 2011, op. cit.

[76] MATESCO, V. R. *Inovação tecnológica das empresas brasileiras*: a diferenciação competitiva e a motivação para inovar. Tese (Doutorado) – Instituto de Economia Industrial, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 1993 apud SANTOS, Adriana B. A. dos; FAZION

Além disso, a partir da década de 1980, devido à globalização da economia e à flexibilização dos formatos organizacionais que envolvem empresas, agências estatais e centros de pesquisa, surgiu um novo foco de análise. A formação e o desenvolvimento de redes passaram a ser tema central das pesquisas acerca de inovação.[77] Thales de Andrade, professor da Faculdade de Ciências Sociais da PUC-Campinas, escreve: [78]

> Nesse contexto, em que a estrutura organizacional assentada nos fluxos de informação passa a ser mais essencial que os próprios produtos desenvolvidos a partir das atividades tecnológicas, estabelece-se um novo conceito, o de sistemas nacionais de inovação. As interações entre os agentes econômicos, as instituições de pesquisa e organismos governamentais estipulam ações recíprocas que geram a capacidade de desenvolvimento de condições de inovação. Políticas locais e setorizadas passam a ser imprescindíveis para a compreensão do potencial inovativo de uma nação e região, independentemente da atividade específica de cada setor e das oscilações da demanda. A interação das firmas com e no sistema passa a adquirir significado estratégico. Essas capacidades, que anteriormente eram consideradas como que mais puramente administrativas ou gerenciais, são consideradas, no período atual, como parâmetros de inovação.

Outra visão sobre a inovação é a perspectiva construtivista da sociologia das técnicas, pela qual os fatores econômicos não determinariam o rumo da inovação, mas apenas o acompanhariam. De acordo com esse entendimento, a escolha de tecnologias seria devida antes à compatibilização entre crenças e interesses de diversos grupos e setores estratégicos da atividade tecnológica do que a critérios puramente econômicos.[79] O contexto social adquire relevância no desenvolvimento do processo inovador. Alguns autores, como Michel Callon[80] e Bruno Latour,[81] apesar de possuírem algumas diferenças de entendimento, foram

---

Cíntia B.; MEROE, Giuliano P. S. de. "Inovação: um estudo sobre a evolução do conceito de Schumpeter", 2011, op. cit., p. 12.

[77] ANDRADE, Thales de. Inovação tecnológica e meio ambiente: a construção de novos enfoques. *Ambiente & Sociedade*, v. VII, n. 1, jan./jun. 2004, p. 91.

[78] Ibid., p. 91-92.

[79] Ibid., 2004, p. 92-93.

[80] CALLON, Michel. Society in the making: the study of technology as a tool for sociological analysis. In: BIJKER, Wiebe E.; HUGHES, Thomas P; PINCH, Trevor F. (Ed.). *The social construction of technological systems*: new directions in the sociology and history of technology. Cambridge, MA: The MIT Press, 1989. p. 83-103.

[81] LATOUR, Bruno. *Ciência em ação*: como seguir cientistas e engenheiros sociedade afora. Trad. Ivone C. Benedetti. São Paulo: Ed. Unesp, 2000. Para o autor, o processo de produção da ciência envolve uma rede de elementos humanos, como cientistas, engenheiros e cidadão comum, e não-humanos, como laboratórios e máquinas, que podem ser observados em contínua interação. Confira-se também: LATOUR, Bruno; WOOLGAR, Steve. *Laboratory life*: the construction of scientific facts. Princeton: Princeton University Press, 1986; FERREIRA, Rubens da Silva.

fundamentais para a elaboração dessa teoria, da qual podemos destacar três princípios: (1) deve-se evitar dar atenção ao inventor de forma isolada; (2) é preciso criticar manifestações de determinismo tecnológico; (3) é necessário combater a dicotomia tecnologia-sociedade, tratando os aspectos técnicos, sociais, econômicos e políticos do processo de inovação de modo integrado.[82-83]

No entanto, é importante ressaltar que, independentemente da posição econômica a ser utilizada, o termo *tecnologia* não deve denotar *per se* uma inovação limitada ao meio digital. O dicionário *Michaelis* assim conceitua *tecnologia*:[84]

> Conjunto de processos, métodos, técnicas e ferramentas relativos a arte, indústria, educação etc. 2. Conhecimento técnico e científico e suas aplicações a um campo particular. 3. Tudo o que é novo em matéria de conhecimento técnico e científico. 4. Linguagem peculiar a um ramo determinado do conhecimento, teórico ou prático. 5. Aplicação dos conhecimentos científicos à produção em geral.

Portanto, dentro do significado denotativo do termo, qualquer uso da técnica ou do conhecimento utilizado para facilitar e aprimorar o trabalho com a arte, indústria e outros instrumentos pode ser considerado como uma nova tecnologia.

A definição da palavra *tecnologia* não explicita por que tendemos, atualmente, a associar a tecnologia com uma inovação no meio digital. Nesse sentido, cabe ressaltar o efeito da variação linguística, que consiste na adaptação do significado de um termo a depender de fatores históricos, culturais ou regionais.

Eric Schatzberg, em seu artigo "Technik comes to America: changing meanings of technology before 1930",[85] demonstra como, no início do século XIX, a palavra *technik* na língua inglesa era associada a um ramo de estudo ligado

---

Ciência e tecnologia no olhar de Bruno Latour. *Inf. Inf.*, Londrina, v. 18, n. 3, p. 275-281, set./dez. 2013.

[82] BENAKOUCHE, Tamara. Tecnologia é sociedade: contra a noção de impacto tecnológico. *Cadernos de Pesquisa*, n. 17, p. 3, set. 1999.

[83] Sobre o tema, confira-se ainda: TRIGUEIRO, Michelangelo Giotto Santoro. O que foi feito de Kuhn? O construtivismo na sociologia da ciência: considerações sobre a prática das novas biotecnologias. In: SOBRAL, Fernanda et al. (Org.) *A alavanca de Arquimedes*: ciência e tecnologia na virada do século. Brasília: Paralelo 15, 1997.

[84] Disponível em: <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=tecnologia>. Acesso em: 27 mar. 2017.

[85] SCHATZBERG, Eric. Technik comes to America: changing meanings of technology before 1930. *Technology and Culture*, v. 47, n. 3, p. 486-512, jul. 2006. Disponível em: <http://muse.jhu.edu/article/201479>. Acesso em: 27 mar. 2017.

às chamadas *practical arts* e não a processos industriais. Isso ocorria porque até esse século, a arte era vista como uma parte do espectro do conhecimento, o qual também englobava a ciência.[86]

O afastamento do termo *technology* em relação à arte ocorreu, de acordo com Schatzberg, por dois fatores principais: (1) o surgimento do conceito de *fine arts*,[87] que não remetia aos trabalhos mais práticos realizado por artesãos, e (2) por conta da Revolução Industrial do século XIX,[88] que necessitava se legitimar diante da nova ordem social e econômica que estava a surgir. Nesse sentido, um afastamento das *mechanical arts* em relação ao trabalho realizado por artesãos foi essencial para aproximar o termo das *applied sciences*, tendo em vista que o conceito do primeiro grupo era incapaz de explicar a realidade que estava a surgir com a Revolução Industrial.

Ao fim do século XIX, por influência dos cientistas sociais alemães, autores como Thorstein Veblen começaram a associar o termo à indústria e à engenharia modernas.[89] Segundo Schatzberg,[90] "os agentes de classe média do industrialismo, incluindo os homens da ciência, usaram a retórica da ciência aplicada para apropriar, ou pelo menos subordinar, o conhecimento artesanal".[91]

Na mesma época, até o significado de *ciência* foi alterado. Antes de 1900, a ciência não se referia a métodos de laboratório ou à busca de leis gerais, mas sim a algo mais amplo, uma espécie de conhecimento sistemático ou pensamento rigoroso, que poderia incluir a maioria das ciências sociais e mesmo a teologia.

No final do século XIX, a crescente profissionalização das disciplinas acadêmicas e o prestígio da tecnologia incentivaram os cientistas naturais a reivindicar o monopólio da ciência. Esse conceito amplo de ciência do século XIX deslocou o conhecimento artesanal, transferindo a valorização dos artesãos para os proprietários de fábricas, inventores e engenheiros.

---

[86] SCHATZBERG, Eric. From art to applied science. *Isis*, v. 103, n. 3, p. 555-563, 2012.
[87] *Fine arts* seria todo tipo de trabalho artístico que fosse fruto da imaginação e da inovação, como a pintura e a poesai; no entanto, o conceito não englobava o trabalho realizado por artesãos.
[88] SCHATZBERG, Eric. "From art to applied science", 2012, op. cit.
[89] Cf. MARX, Leo. Technology – The Emergence of a Hazardous Concept. *Technology and Culture*, v. 51, n. 3, p.561-577, jul. 2010.
[90] Ibid.
[91] Tradução livre do autor. No original: "*middle-class agents of industrialism, including men of science, used the rhetoric of applied science to appropriate, or at least subordinate, artisanal knowledge*".

Antes da primeira década do século XX, *tecnologia* era um termo obscuro quase universalmente definido como a "ciência das artes", com "ciência" aqui entendida primeiramente como um sistema de classificação. No entanto, a conexão com a ciência aplicada, segundo Schatzberg, estava lá desde o início. A tecnologia era uma ciência que dizia respeito às artes úteis. Os engenheiros americanos, em particular, basearam sua reivindicação de *status* social no conceito de ciência aplicada como um corpo de conhecimento autônomo, enquanto os cientistas poderiam usar a definição de ciência aplicada como o emprego da ciência pura para reivindicar o crédito pelas maravilhas modernas da idade industrial.[92]

Tendo em vista a conexão feita entre tecnologia e ciência, interessante observar no que esta consiste, sobretudo por conta da multiplicidade de significados conferidos à palavra. Observe o que leciona José Ferrater Mora[93]:

> O substantivo *scientia* procede do verbo *scire*, que significa 'saber'. Entretanto, não é recomendável ater-se a essa equivalência, pois há saberes que não pertencem à ciência: por exemplo, o saber que às vezes se qualifica de comum, ordinário ou vulgar. Sabem-se, com efeito, muitas coisas que ninguém ousaria apresentar como se fossem enunciados científicos. (...) Parece necessário, portanto, definir que tipo de saber é o científico. Várias respostas nos ocorrem. Por exemplo: que é um saber culto ou desinteressado, que é um saber teórico, suscetível de aplicação prática e técnica, que é um saber rigoroso e metódico etc. Todas essas respostas nos proporcionam alguma informação sobre o tipo especial do saber científico, mas não são suficientes; têm, além disso, um inconveniente, em nosso caso importante: não permitem distinguir a ciência e a filosofia. (...) É comum considerar a ciência como um modo de conhecimento que visa formular, mediante linguagens rigorosas e apropriadas – na medida do possível, com o auxílio da linguagem matemática –, leis por meio das quais são regidos os fenômenos.

Neste sentido, a ciência se distingue da filosofia, pois, dentre outras diferenças, enquanto o objetivo daquela é ser um modo de conhecer referente ao ser e que nos dá informações detalhadas sobre a sociedade, a filosofia é um modo de viver ligado ao dever ser e que constrói e descontrói elaborações sobre sistemas[94].

---

[92] SCHATZBERG, Eric. "From art to applied science", 2012, op. cit.

[93] MORA, José Ferrater. *Dicionario de Filosofia*, tomo I (A-D). 2. ed. ver., aum. e atual. por Josep-Maria Terricabras. São Paulo: Edições Loyola, 2004, p. 457.

[94] Confira-se as distinções entre ciência e filosofia apontadas por José Ferrater Mora: "1) *a*1) A ciência progride e nos informa, de modo cada vez mais completo e detalhado, sobre a realidade, enquanto a filosofia não progride, porque é um incessante tecer e destecer de sistemas. *b*1) A ciência é um modo de conhecer, enquanto a filosofia é um modo de viver. *c*1) A ciência refere-se

Veblen foi um dos primeiros sociólogos a dar um novo significado à palavra *tecnologia*. Seu principal argumento era que o conhecimento tecnológico não é restrito apenas a algumas comunidades humanas, estando presente, inclusive, nos grupos considerados mais primitivos. Esse tipo de conhecimento constituía, para o autor, o *immaterial equipment of production*, uma espécie de oposto ao equipamento material da indústria, como ferramentas e máquinas. Nas comunidades humanas, o conhecimento tecnológico seria produzido coletivamente. Contudo, à medida que os insumos foram se tornando escassos, os indivíduos capazes de tê-los os utilizaram como um meio de controle desse conhecimento tecnológico coletivo, criando, assim, as bases de um domínio pecuniário voltado para o conhecimento tecnológico.[95] Veblen utilizou essa tese como um ponto central de sua crítica ao capitalismo moderno.[96]

Durante a década de 1920, poucos acadêmicos corroboraram o significado dado por Veblen para o termo *tecnologia*. No entanto, eles também passaram a se influenciar pela matriz social alemã. Tal fato pode ser percebido porque foram atribuídos ao termo *technology* significados equivalentes a *technik* ou *industrial arts* durante esse período.

Na década de 1930, essa aproximação do termo *tecnologia* com sua equivalente alemã, *technik*, continuou. Contudo, o significado atribuído durante o século XIX, *science of the arts*, não se perdeu de imediato. Durante esse período, tecnologia passou a significar um híbrido entre *science of the arts* e *applied science*. Essa confusão polissêmica auxiliou na disseminação da ideia, capitaneada por Charles Beard, de que as mudanças tecnológicas, necessariamente, estão

---

ao ser; a filosofia, ao dever ser ou, em geral, ao valor. *d*1) A ciência é conhecimento rigoroso; a filosofia, concepção do mundo exprimível igualmente mediante a religião ou a arte. Por isso, a ciência está de um lado, enquanto a filosofia (com a religião e a arte) está de outro (às vezes considerado oposto). (...) *f*1) A ciência opera mediante observação, experimentação, inferência e dedução, enquanto a filosofia opera mediante inuição. Como consequência disso, a ciência refere-se somente ao fenômeno, enquanto a filosofia atinge o numênico etc. (...) 3) *a*3) A relação entre a filosofia e a ciência é o tipo histórico: a filosofia foi e continuará sendo a mãe das ciências, por ser a disciplina que se ocupa da formação de problemas, depois tomados pela ciência para ser solucionados." (MORA, José Ferrater. *Dicionario de Filosofia*, tomo I (A-D). 2. ed. ver., aum. e atual. por Josep-Maria Terricabras. São Paulo: Edições Loyola, 2004, p. 457)."

[95] Ibid.

[96] Cf. MARX, Leo. Technology: the emergence of a hazardous concept. *Technology and Culture*, v. 51, n. 3, p. 561-577, 2010.

atreladas a descobertas científicas.[97] Para Eric Schatzberg essa associação teve um impacto relevante, como demonstrado na seguinte passagem:[98]

> Desde os primeiros anos da República Americana, oradores, editorialistas e intelectuais abraçaram as maravilhas tecnológicas de seu tempo como manifestações visíveis do progresso. Como historiador americano, Beard conhecia intimamente essa retórica. A novidade de Beard residia em vincular explicitamente o termo *tecnologia* à ideia de progresso de uma maneira que tornou a própria tecnologia a força motriz da história.[99]

Ronald Kline,[100] por sua vez, argumenta que foram dados diversos significados ao termo *applied sciences* ao longo do tempo (especificamente entre 1880 e 1945), desde ideias ligadas ao conceito de *useful arts* até questões relacionadas à engenharia e conhecimento técnico. Segundo o autor, tais significados seriam o que chamamos hoje de *science and technology.*

É necessário esclarecer que não há uma diferença significativa entre os termos *useful arts e practical arts*, tendo em vista que ambos remetem ao trabalho manual realizado por artesãos. No entanto, ainda que tais expressões fossem consideradas sinônimos de *technology* no século XIX, o mesmo não pode ser dito em relação ao significado desse termo a partir do século XX. Esse é o ponto ressaltado por alguns historiadores da tecnologia[101] que indicam que a diferença entre esses dois conceitos passou a existir tanto em nível material quanto em nível linguístico.[102]

---

[97] SCHATZBERG, Eric. "From art to applied science", 2012, op. cit.
[98] Ibid.
[99] Tradução livre do autor. No original: "*From the early years of the American Republic, orators, editorialists, and intellectuals embraced the technological marvels of their day as visible manifestations of progress. As an American historian, Beard knew this rhetoric intimately. Beard's novelty lay in explicitly linking the term technology to the idea of progress in a way that made technology itself the motive force of history*".
[100] KLINE, R. Construing "technology" as "applied science": public rhetoric of scientists and engineers in the United States, 1880-1945. *Isis*, v. 86, n. 2, p. 194-221, jun. 1995. Disponível em: <www.jstor.org/stable/pdf/236322.pdf>. Acesso em: 28 mar. 2017.
[101] OLDENZIEL, R. Introduction: signifying semantics for a history of technology. *Technology and Culture*, v. 47, n. 3, p. 477-485, jul. 2006. Disponível em: <www.jstor.org/tc/accept?origin=/stable/pdf/40061168.pdf>. Acesso em: 5 jan. 2017; LERMAN, N. The uses of useful knowledge: science, technology, and social boundaries in an industrializing city. *Osiris*, v. 12, p. 39-59, 1997. Disponível em: <www.jstor.org/stable/pdf/301898.pdf>. Acesso em: 5 jan. 2017.
[102] Na perspectiva material, a alteração de significado da palavra *technology* se deu por conta da primeira revolução industrial. Com o advento das máquinas a vapor, a produção passou a ser em massa, padronizada e célere, o que tornou o trabalho realizado por artesãos na produção de manufaturas facilmente substituível. A evolução linguística se deu não só pelo uso do conceito de *fine arts* ainda no século XVIII, como também pelo uso da palavra alemã *Technik*, que se aproximava das ações realizadas no campo científico e industrial.

Para Leo Marx,[103] a palavra *tecnologia* preencheu um vácuo semântico caracterizado por uma série de circunstâncias sociais para as quais não havia um conceito adequado. As ideias de *useful arts* e de *mechanical arts* passaram a ser tidas como algo pejorativo e inferior face às *high* ou *fine arts*. Essas noções não eram mais suficientes sob a ótica ideológica e nem sob a ótica substantiva em virtude da relação que se fez entre inovação na ciência, *mechanic arts* e crença no progresso. Tecnologia, por sua vez, vai além de um simples meio para atingir o progresso. Nas palavras do autor:[104]

> O que faltava, do ponto de vista ideológico, era o conceito de uma forma de poder - de progresso - que excedia, em grau, escopo e escala, a capacidade relativamente limitada das artes meramente úteis (ou mecânicas ou práticas) para gerar mudanças sociais. O que era necessário era um conceito que não significava apenas, como as artes úteis, um meio de alcançar o progresso, mas sim um que significava uma entidade discreta que, em si mesma, constituía um progresso virtualmente constituído. Além disso, a idéia de utilidade havia trazido o selo da vulgaridade. Desde a antiguidade, as artes úteis em suas várias formas foram consideradas intelectual e socialmente inferiores às *high arts* (ou *fine*, criativas ou imaginativas). O conceito de artes úteis e suas variantes implicaram – se apenas porque ele explicitamente designou um ramo subordinado da entidade abrangente, as artes – uma categoria limitada e limitativa. Na verdade, a distinção entre as artes úteis e as artes plásticas tinha servido para ratificar um conjunto de distinções invioláveis entre coisas e idéias, o físico e o mental, o mundano e o ideal, corpo e alma, feminino e masculino, fazer e pensar, o trabalho de homens escravizados e de homens livres. Ao associar a ferrovia com ciência, negócios e riqueza, Webster e seus contemporâneos criaram a necessidade de um termo que apague esse legado depreciativo e colocam o útil em um plano intelectual e social mais elevado. (...) Todos esses propósitos ideológicos foram atendidos pelo relativamente abstrato, indeterminado, neutro e sintético termo *tecnologia*. Enquanto as artes mecânicas chamavam a atenção para os homens com mãos sujas trabalhando em bancos de trabalho, a tecnologia evoca imagens de técnicos masculinos (...) limpos e bem-educados em cabines de controle olhando para controladores, painéis de instrumentos ou monitores de computador. E tendo em vista que as artes mecânicas eram consideradas como pertencentes à esfera mundana do trabalho cotidiano, fisicalidade e praticidade – de artesanatos e habilidades artesanais – a tecnologia é identificada com o domínio social e intelectual mais elevado da universidade. Esta palavra abstrata, com seu vazio vívido, a falta de um referente específico artefactual, tangível e sensível, sua aura de sanitização, cerebração e precisão sem sangue, ajudou a facilitar a introdução das artes práticas - especialmente a nova profissão de engenharia - no recinto da aprendizagem superior.[105]

---

[103] MARX, Leo. Technology: the emergence of a hazardous concept. *Social Research*, v. 64, n. 3, p. 965-988, 1997.

[104] Ibid. p. 977-978, 1997.

[105] Tradução do autor. Lê-se, no original: "*What was missing, from an ideological standpoint, was the concept of a form of power - of progress - that far exceeded, in degree, scope, and scale, the relatively limited capacity of the merely useful (or mechanic or practical or industrial) arts to generate social change. What was needed was a concept that did not merely signify, like the useful*

A utilização do termo começou a ser feita no século XIX, quando se referia a um tipo de manual e também a *mechanic arts* sob a ótica coletiva. Contudo, foi apenas no século XX, sobretudo após a Primeira Guerra Mundial, que o vocábulo tecnologia, que é vago, intangível e, de certa forma, indeterminado, teve seu uso expandido. Ele não se refere apenas a coisas específicas ou tangíveis, como uma ferramenta ou uma máquina, e vai ao encontro do amálgama que surgiu à época entre ciência e indústria. O componente material torna-se apenas mais um dos elementos constitutivos da tecnologia.

Pela multiplicidade de associações que foram feitas ao termo *tecnologia* ao longo dos séculos XIX e XX, o campo de estudo da história da tecnologia se tornou grande e diversificado. John. M. Staudenmaier argumenta que existem nove áreas centrais de estudo relacionadas à história da tecnologia, e quatro assuntos principais nesses campos. Um dos tópicos mais comuns seria o que trata da *technological creativity*.[106]

> Entre as décadas de 1950 e 1970, existia um ponto em comum nos estudos sobre esse tema, que identificavam três tipos de atividade criativa diferentes no surgimento das novas tecnologias. A primeira seria a invenção, a qual teria como foco a solução de problemas técnicos. A segunda seria o desenvolvimento, que se consubstancia na criação de protótipos funcionais por meio de testes em ambientes controlados. Por fim, haveria a inovação, que seria representada pela

---

arts, a means of achieving progress, but rather one that signified a discrete entity that, in itself, virtually constituted progress. Besides, the idea of utility had long borne the stamp of vulgarity. Ever since antiquity, the useful arts in their various guises, had been regarded as intellectually and socially inferior to the high (or fine, creative, or imaginative) arts. The concept of the useful arts and its variants implied, if only because it explicitly designated a subordinate branch of the all-inclusive entity, the arts, a limited and limiting category. Indeed, the distinction between the useful and the fine arts had served to ratify a set of invidious distinctions between things and ideas, the physical and the mental, the mundane and the ideal, body and soul, female and male, making and thinking, the work of enslaved men and that of free men. By associating the railroad with science, business, and wealth, Webster and his contemporaries created the need for a term that would erase this derogatory legacy and elevate the useful to a higher intellectual and social plane.

All of these ideological purposes, and more, were served by the relatively abstract, indeterminate, neutral, synthetic-sounding term technology. Whereas the mechanic arts called to mind men with soiled hands tinkering at workbenches, technology conjures up images of clean, well-educated, (...) male technicians in control booths gazing at dials, instrument panels, or computer monitors. And whereas the mechanic arts were thought of as belonging to the mundane world of everyday work, physicality, and practicality - of humdrum handicrafts and artisanal skills - technology is identified with the more elevated social and intellectual realm of the university. This abstract word, with its vivid blankness, its lack of a specific artifactual, tangible, sensuous referent, its aura of sanitized, bloodless cerebration and precision, helped to ease the introduction of the practical arts - especially the new engineering profession - into the precincts of the higher learning."

[106] STAUDENMAIER, John M. Recent trends in the history of technology. *The American Historical Review*, v. 95, n. 3, p. 715-725, jun. 1990.

> junção do marketing e do processo de fabricação do produto nas indústrias, ambos voltados na criação de tecnologias capazes de serem utilizadas cotidianamente pelas pessoas.[107-108]

O conceito de novidade e aplicação industrial e a atividade inventiva são até hoje pré-requisitos para o enquadramento de uma criação intelectual como invenção.[109] Somente as criações que cumprirem esses pré-requisitos poderão ser atestadas como invenções pelo INPI, órgão responsável, no Brasil, por registrar os pedidos envolvendo criações industriais (além de *software*) e emitir a carta-patente que concede, a título constitutivo (e não declaratório), o monopólio de exploração temporário sobre a criação intelectual.

Segundo estudo do Massachusetts Institute of Technology (MIT), as invenções, como ícones da produção de novas tecnologias, podem ser caracterizadas de duas formas: (1) microinvenções ou invenções disruptivas que modificam a sociedade de uma forma significativa e (2) microinvenções, relacionadas ao processo de aprimoramento e modificações de produtos, os quais, com o tempo, podem ampliar a área de atuação do produto inicial.[110] Esse processo, no entanto, tem de ser capaz de criar algo útil e que não seja previamente conhecido.

De acordo com o economista Nathan Rosenberg, de Stanford, quanto a boa parte das inovações tecnológicas disruptivas, no momento em que foram criadas, não se tinha uma visão clara de qual seria sua área de aplicação ou potencial de utilidade.

---

[107] Tradução livre do autor. No original: "*From the late 1950s into the 1970s, most work in this area argued that three distinctly different modes of creative activity are almost always operative when new technologies emerge: invention (solutions to technical problems), development (high-cost, controlled-environment projects aimed at the creation of a functioning prototype), and innovation (procedures such as manufacturing and marketing, required to introduce the technology into ordinary use).*"

[108] Ibid., p. 717.

[109] BRASIL, *Lei no 9.279, de 14 de maio de 1996*. Regula direitos e obrigações à propriedade industrial. Brasília: Diário Oficial da União (DOU). Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9279.htm>; . Acessado em 02 dez. 2017.

[110] THE LEMELSON-MIT PROGRAM. *Historical perspectives on inventions & creativity*. Workshop realizado pela escola de engenharia do Massachusetts Institute of Technology (MIT), 2003. Disponível em: <http://web.mit.edu/monicaru/Public/old%20stuff/For%20Dava/Grad%20Library.Data/PDF/history-3289136129/history.pdf>. Acesso em: 28 mar. 2017.

Para Rosenberg,[111] "muitas vezes, as invenções têm aplicações poderosas em contextos totalmente imprevistos ou em diferentes setores da economia, e o processo de mapeamento de invenções para aplicações em diferentes domínios envolve [...] 'fluxos intersetoriais'".

Essa atuação não esperada das invenções cria um cenário em que, a depender do contexto histórico, a aplicação de determinada inovação tem outro significado. Um exemplo trazido pelo autor é o do *laser*. Rosenberg argumenta que, em 1950, quando o *laser* foi criado, ele teria sido aplicado somente em pesquisas científicas. Com o tempo, essa invenção passou a ser utilizada em um amplo rol de áreas acadêmicas, em procedimentos médico-cirúrgicos, bem como em processos de leitura digital em aparelhos eletrônicos.[112]

Nesse sentido, é necessário dizer que a utilidade de determinado produto tecnológico nem sempre pode ser derivada previamente. É possível que, para defini-la, seja necessário racionalizar de qual sentido de utilidade se está a tratar. Tal como posto por Ruth Oldenziel,[113] a tecnologia, nos termos atuais, não pode ser compreendida como um meio ligado às artes, o que distancia o conceito do aspecto subjetivo da utilidade e do desejo individual. No entanto, se pensarmos em utilidade a partir de teorias utilitaristas, mesmo um sensor que anuncia o tipo de bebida que se está a beber pode ser considerado socialmente útil, tendo em vista os recursos econômicos que são gerados direta e indiretamente com sua venda.

Por fim, vale dizer que, ainda que os termos *invenção*, *inovação* e *tecnologia* não estivessem, desde sua origem, necessariamente relacionados, no imaginário da sociedade moderna eles são compreendidos cada vez mais dentro de um mesmo contexto.

Por essa razão, é necessário compreender o significado de cada um desses termos, conforme explicado neste capítulo, tendo em vista que, sem tal reconstrução histórica, não seria possível entender o porquê da sua associação ao

[111] Tradução livre do autor. No original: "*Often, inventions have powerful applications in totally unanticipated contexts or in different sectors of the economy, and the process of mapping inventions to applications in different domains involves what Rosenberg calls 'intersectoral flows'*" (THE LEMELSON-MIT PROGRAM. Historical perspectives on inventions & creativity, 2003, op. cit., p. 35).
[112] Ibid.
[113] OLDENZIEL, R. "Introduction: signifying semantics for a history of technology", 2006, op. cit.

que há de mais moderno na sociedade, bem como aos setores científicos e industriais. No limite, o significado do termo *tecnologia* desemboca em uma discussão em relação aos aspectos sociais, econômicos e culturais de uma determinada sociedade em um determinado contexto histórico.

Dessa forma, apesar de considerarmos hoje, em grande medida, *tecnologia* "sinônimo de aparelhos cada vez mais inteligentes, sofisticados e rápidos, como seu computador, *tablet* ou *smartphone*", há quem diga que não é errado considerar "que um arco e flecha, por exemplo, também sejam tecnologia".[114]

Essa digressão é fundamental para refletirmos sobre a concepção que temos hoje de IoT[115] e dos variados produtos que surgem desse contexto, muitas vezes desacoplados do caráter de real utilidade e novidade, mas que, ainda assim, são considerados tecnologias inovadoras somente pelo fato de envolverem o aspecto digital.

A expressão IoT é utilizada para designar a conectividade e interação entre vários tipos de objetos do dia a dia, sensíveis à Internet.[116] 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".[117] 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.[118]

Do ponto de vista da normalização técnica, a IoT pode ser vista como uma infraestrutura global voltada para a era digital, permitindo serviços avançados por

[114] Cf. KARASINSKI, Lucas. "O que é tecnologia?", 2013, op. cit.
[115] Cf. BURRUS, Daniel. The Internet of things is far bigger than anyone realizes. *Wired*, [s.d.]. Disponível em: <www.wired.com/2014/11/the-Internet-of-things-bigger/>. Acesso em: 29 mar. 2017; MATTERN, Friedemann; FLOERKEMEIER, Christian. *From the Internet of computers to the Internet of things*. [s.d.]. Disponível em: <www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf>. Acesso em: 29 mar. 2017.
[116] 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, Setúbal, 2016.
[117] Cf. NASCIMENTO Rodrigo, O que, de fato, é Internet das coisas e que revolução ela pode trazer? *Computerworld*, 12 mar. 2015. Disponível em: <http://computerworld.com.br/negocios/2015/03/12/o-que-de-fato-e-Internet-das-coisas-e-que-revolucao-ela-pode-trazer/>. Acesso em: 29 mar. 2017.
[118] Ibid.

meio da interconexão de coisas (físicas e virtuais) com base nas tecnologias de informação e comunicação interoperáveis existentes e em constante evolução.[119]

A discussão sobre objetos conectados está presente desde os primórdios das tecnologias de informação.[120] Bill Joy, cofundador da Sun Microsystems, já na década de 1990, refletia sobre a conexão de dispositivo para dispositivo (*device to device* – D2D), pensando em um tipo de conexão que engloba não apenas uma rede, mas "várias webs".[121-122]

Kevin Ashton, do MIT, em 1999, propôs o termo *Internet das coisas*. Dez anos após apresentar essa expressão, escreveu o artigo "A coisa da Internet das coisas"[123] para o *RFID Journal*, reforçando o vocábulo. De acordo com Ashton, as pessoas necessitam conectar-se com a Internet por meio de variadas formas devido à falta de tempo proporcionada pela rotina do novo cotidiano.

Dessa forma, segundo Ashton, deverá ser possível armazenar dados, até sobre o movimento dos nossos corpos, com uma precisão cada vez mais acurada. Para o pesquisador, essa revolução será maior do que o próprio desenvolvimento do mundo *online* que conhecemos hoje. Tais registros serão úteis, na visão de Ashton, por exemplo, para a economia de recursos naturais e energéticos, e também para possíveis facilidades pessoais e de saúde. Muitas dessas utilidades já estão em vigor, e as funcionalidades da IoT são possíveis graças a tecnologias como *wi-fi*, *bluetooth* e identificação por radiofrequência RFID.[124-125]

---

[119] SANTUCCI, Gérald. *The Internet of things*: between the revolution of the Internet and the metamorphosis of objects. Disponível em: <http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-between-the-Internet-revolution.pdf>. Acesso em: 29 mar. 2017.

[120] LEINER, Barry M. et al. Brief history of the Internet. *Internet Society*, [199-?]. Disponível em: <www.Internetsociety.org/Internet/what-Internet/history-Internet/brief-history-Internet>. Acesso em: 29 mar. 2017.

[121] PONTIN, Jason. ETC: Bill Joy's six webs. *MIT Technology Review*, 29 set. 2005. Disponível em: <www.technologyreview.com/view/404694/etc-bill-joys-six-webs/>. Acesso em: 29 mar. 2017.

[122] HAPGOOD Fred. 20 years of IT history: connecting devices, data and people. *CIO*, 28 set. 2007. Disponível em: <www.cio.com/article/2438016/infrastructure/20-years-of-it-history--connecting-devices--data-and-people.html>. Acesso em: 29 mar. 2017.

[123] ASHTON, Kevin. That 'Internet of Things' Thing. *RFID Journal*, 22 jun. 2009. Disponível em: <www.rfidjournal.com/articles/view?4986>. Acesso em: 29 mar. 2017.

[124] "Para ligar os objetos e aparelhos do dia a dia a grandes bases de dados e redes e à rede das redes, a Internet, é necessário um sistema eficiente de identificação. Só desta forma se torna possível coligir e registar os dados sobre cada uma das coisas. A identificação por rádio frequência RFID oferece esta funcionalidade. Segundo, o registo de dados beneficiará da capacidade de detectar mudanças na qualidade física das coisas usando as tecnologias sensoriais (sensor technologies). A tecnologia RFID que usa frequências de rádio para identificar os produtos é vista como potenciadora da Internet das Coisas. A tecnologia RFID que usa frequências de rádio para

Os objetos inteligentes e interconectados podem efetivamente nos ajudar na resolução de problemas reais. Do ponto de vista dos consumidores, os produtos que hoje estão integrados com a tecnologia da IoT são das mais variadas áreas e possuem funções diversas, desde eletrodomésticos,[126] meios de transporte, até brinquedos.

Existem também, hoje, as peças de vestuário que possuem conectividade de IoT, fazendo parte de uma categoria denominada *wearables*. Essas tecnologias vestíveis consistem em dispositivos que estão conectados uns aos outros produzindo informações sobre os usuários e as pessoas ao redor deles. Entre os principais produtos se destacam as pulseiras e tênis que monitoram a atividade física do usuário, além de relógios e óculos inteligentes que pretendem prover ao usuário uma experiência de imersão na própria realidade.[127]

Para diferenciar os produtos da IoT por sua utilidade, alguns estudos vêm sendo desenvolvidos nesse tema utilizando-se da diferenciação entre *Internet das coisas úteis* e *Internet das coisas inúteis*. Produtos incomuns, como garrafas térmicas com sensores, geladeiras com Twitter e persianas conectadas, estariam

---

identificar os produtos é vista como potenciadora da Internet das Coisas. Embora algumas vezes identificada como a sucessora dos códigos de barras os sistemas RFID oferecem para além da identificação de objectos informações importantes sobre o seu estado e localização". Vide: A INTERNET DAS coisas é a extensão da Internet ao mundo físico em que torna-se possível a interação com objetos e a própria comunicação autônoma entre objetos. *ActivaiD*, [s.d.]. Disponível em: <www.rfid.ind.br/Internet-das-coisas#.VagXS_lVhHw>. Acesso em: 29 mar. 2017; RFID-COE. *O que é RFID*, [s.d.]. Disponível em: <www.rfid-coe.com.br/_Portugues/OqueERFID.aspx>. Acesso em: 29 mar. 2017; LIMA, Leonardo. RFID e privacidade? Experiências derrubam alguns mitos. *Cabtec GTI*, jul. 2014. Disponível em: <www.gradeti.com.br/blog/rfid/2014/07/rfid-e-privacidade-experiencias-derrubam-alguns-mitos/>. Acesso em: 29 mar. 2017.

[125] A tecnologia RFID é essencial para intensificação da Internet das coisas no cotidiano, sendo utilizada na identificação de objetos, disponibilizando informações sobre o estado, a localização e mudanças no ambiente dos aparelhos equipados.

[126] "Geladeiras inteligentes são talvez o mais comum dos exemplos quando falamos sobre Internet das Coisas. O refrigerador Samsung RF28HMELBSR/AA, por exemplo, é equipado com uma tela LCD capaz de reproduzir a tela de seu smartphone no refrigerador. É possível reproduzir vídeos e músicas, consultar a previsão do tempo e até mesmo fazer compras online enquanto verifica na geladeira os itens que precisam ser comprados. O refrigerador traz ainda um app chamado Epicurious, que permite a consulta de receitas online" (NASCIMENTO, Rodrigo. "O que, de fato, é Internet das coisas e que revolução ela pode trazer?", 2015, op. cit.).

[127] Confira-se LANDIM, Wikerson. Wearables: será que esta moda pega? *Tec Mundo*, jan. 2014. Disponível em: <www.tecmundo.com.br/tecnologia/49699-wearables-sera-que-esta-moda-pega-.htm>. Acesso em: 31 jan. 2017; DARMOUR, Jennifer. The Internet of you: when wearable tech and the Internet of things collide. *Artefact Group*, [s.d.] Disponível em: <www.artefactgroup.com/articles/the-Internet-of-you-when-wearable-tech-and-the-Internet-of-things-collide/>. Acesso em: 29 mar. 2017; O'BRIEN, Ciara. Wearables: Samsung chases fitness fans with gear fit 2. *The Irish Times*, ago. 2016. Disponível em: <www.irishtimes.com/business/technology/wearables-samsung-chases-fitness-fans-with-gear-fit-2-1.2763512>. Acesso em: 29 mar. 2017.

no rol de coisas que possivelmente se contrapõem à *Internet das coisas úteis*, termo difundido pelo blog de tecnologia *MeioBit.*[128]

Para fazer essa distinção de acordo com o potencial de utilidade, a *Trendwatching*,[129] newsletter sobre consumo e negócio, delimita a IoT de acordo com as seguintes áreas: saúde, física e mental; bem-estar; segurança pessoal; privacidade de dados. Já a empresa Libelium,[130] vinculada ao mercado de IoT, em 2013 fez essa distinção dividindo a IoT em 12 segmentos: cidades, meio ambiente, água, medição, segurança e emergências, comércio, logística, controle industrial, agricultura, pecuária, automação residencial e saúde.

O conceito de *Internet das coisas inúteis* relaciona-se ao posicionamento crítico sobre a adaptação de tecnologias avançadas em objetos sem que haja necessidade para tanto, visto que tornar um objeto inteligente sem necessidade pode complicar seu uso e encarecer o produto desnecessariamente, inexistindo um aprimoramento útil. Em diversos casos, o objeto analógico mais simples, sem tecnologia avançada envolvida, atende suficientemente ao consumidor, sem necessidade de ser algo *high tech*, podendo custar menos e ter uma utilização facilitada.

A tecnologia digital não necessariamente torna a vida das pessoas mais fácil.[131] Os custos para conectar um dispositivo são altos e os benefícios talvez sejam baixos demais para compensar o aumento de valor no produto. Podemos citar como exemplo o *egg minder*,[132] que consiste em uma bandeja com sensor que informa quantos ovos existem na geladeira. De fato, poderia ser valiosa essa informação durante as compras no mercado. No entanto, uma solução de baixo custo como uma lista de compras acabaria sendo menos oneroso, substituindo um

[128] Confira-se a página. Disponível em: <http://meiobit.com/>. Acesso em: 29 mar. 2017.
[129] Cf. INTERNET OF caring things. *Trend Watching*, abr. 2014. Disponível em: <http://trendwatching.com/trends/Internet-of-caring-things/>. Acesso em: 31 jan. 2017.
[130] 50 sensor applications for a smarter world. Get inspired! *Libelium*, 2 maio 2012. Disponível em: <www.libelium.com/50_sensor_applications/>. Acesso em: 29 mar 2017.
[131] KOBIE, Nicole. The useless side of the Internet of things. *Motherboard*, 5 fev. 2015. Disponível em: <http://motherboard.vice.com/read/the-useless-side-of-the-Internet-of-things>. Acesso em: 29 mar. 2017.
[132] CARDOSO, Carlos. A Internet das coisas inúteis: egg minder. *Meio Bit*, nov. 2013. Disponível em: <http://meiobit.com/271383/thinkgeek-egg-minder-smart-bandeja-pra-ovo/>. Acesso em: 31 jan. 2017.

dispositivo caro, com configurações complexas e baterias que precisam ser recarregadas constantemente.[133] Isso não parece tão inteligente.

Fazendo uma crítica à adoção impensada das novas tecnologias, Leo Marx desconstrói a ideia de que tecnologias aprimoradas são necessariamente úteis e conduzem ao progresso da sociedade. Segundo o autor em seu artigo intitulado "*Does Improved Technology Mean Progress?*":[134]

> Melhorar a tecnologia significa progresso? Sim, certamente poderia significar exatamente isso. Mas somente se estivermos dispostos e aptos a responder à próxima pergunta "progresso em direção a quê? O que queremos que nossas novas tecnologias realizem? O que queremos além de metas tão imediatas e limitadas quanto alcançar eficiências, reduzir custos financeiros e eliminar elemento humano problemático de nossos locais de trabalho? Na ausência de respostas a essas perguntas, as melhorias tecnológicas podem muito bem se tornar incompatíveis com o progresso genuíno, isto é, social.[135]

Em complemento, sob o pornto de vista dos consumidores, aduz Estéfano Veraszto (et al.):[136]

> Há ainda uma certa "aura" de poder pelo uso das inovações tecnológicas, não apenas entre países, mas também entre pessoas comuns: comprar algum equipamento novo com mais funções e com mais recursos, que efetivamente não serão usados, pode satisfazer certos impulsos "fetichistas" de consumo e de exercício de uma supremacia, frente aos seus pares.

Outro problema grave envolve a quantidade de lixo oriunda do descarte de objetos e dispositivos obsoletos. O que vem sendo chamado de *e-waste* tende a aumentar no mundo inteiro, pois a conectividade dos aparelhos tende a deixá-los ultrapassados mais rapidamente do que produtos não inteligentes.[137] Segundo

---

[133] EINSTEIN, Ben. The Internet of (dumb) things. *Bolt*, fev. 2014. Disponível em: <https://blog.bolt.io/the-Internet-of-dumb-things-49d102018e16#.9ljsxiy4m>. Acesso em: 31 jan. 2017.

[134] MARX, Leo. Does Improved Technology Mean Progress?. Disponível em: http://w3.salemstate.edu/~cmauriello/Course%20Development/IDS271%20Readings/Marx-Does%20Improved%20Technology%20Mean%20Progress.pdf.

[135] Traducao livre do autor. No original: Does improve technology mean progress? Yes, it certainly could mean just that. But only if we are willing and able to answer the next question" progress toward what? What is that we want our new technologies to accomplish? What do we want beyond such immediate, limited goals as achieving efficiencies, decreasing financial costs, and eliminating the troubling human element from our workplaces? In the absence of answers to these questions, technological improvements may very well turn out to be incompatible with genuine, that is to say social, progress.

[136] VERASZTO, Estéfano Vizconde et al. Tecnologia: buscando uma definição para o conceito. *Prisma.com*, n. 7, p. 60-85, 2008. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/viewFile/681/pdf>. Acesso em: 2 maio 2017.

[137] HOWER, Mike. As "Internet of things" grows, so do E-waste concerns. *Sustainable Brands*, 29 dez. 2014. Disponível em:

pesquisadores da Université Catholique de Louvain, na Bélgica, por exemplo, o mercado de IoT enfrenta desafios para encontrar uma maneira sustentável de descartar o lixo tóxico a ser produzido em larga escala.[138]

Esse problema é acentuado pela rápida perda de interesse nas "coisas inúteis". Pesquisas[139] mostram que metade dos *fitness trackers*, muito comuns no estágio atual do mercado de IoT, não são mais usados. O motivo já é conhecido: esses dispositivos simplesmente não produzem benefícios substanciais que justifiquem amplo engajamento e uso duradouro,[140] contribuindo para o já mencionado *e-waste.*[141]

Além disso, como veremos à frente, transformar um objeto analógico em inteligente, além de encarecer o produto e deixá-lo sujeito a falhas que não teria *a priori*, pode gerar riscos também em relação à segurança e privacidade.[142] Estamos falando de um contexto que envolve, conforme já mencionamos, um volume massivo de dados (*Big Data*) sendo processado, na escala de bilhões de dados diariamente, permitindo que seja possível conhecer cada vez mais os

---

<www.sustainablebrands.com/news_and_views/waste_not/mike_hower/Internet_things%E2%80%99_grows_so_do_e-waste_concerns>. Acesso em: 31 jan. 2017; ADVANCED MP. Environmental impact of IoT. *Advanced MP,* [s.d.] Disponível em: <www.advancedmp.com/environmental-impact-of-iot/>. Acesso em: 31 jan. 2017.

[138] LOUCHEZ, Alain; THOMAS, Valerie. E-waste and the Internet of things. *ITU News*, 2014. Disponível em: <http://itunews.itu.int/en/4850-E-waste-and-the-Internet-of-Things.note.aspx>. Acesso em: 31 jan. 2017.

[139] BRILL, Mark. The Internet of useless things and how to avoid it. *SlideShare*, jun. 2015b. Disponível em: <http://pt.slideshare.net/MarkBrill/the-Internet-of-useless-things-and-how-to-avoid-it>. Acesso em: 31 jan. 2017; BRILL, Mark. Are smartwatches the new sandwich toaster? *Brands, Innovation and Creative Technologies*, 27 mar. 2015a. Disponível em: <https://brandsandinnovation.com/2015/03/27/are-smartwatches-the-new-sandwich-toaster/>. Acesso em: 30 jan. 2017; MADDOX, Teena. Wearables have a dirty little secret: 50% of users lose interest. *Tech Republic*, 13 fev. 2014. Disponível em: <www.techrepublic.com/article/wearables-have-a-dirty-little-secret-most-people-lose-interest/>. Acesso em: 30 jan. 2017; SMARTWATCH OWNERSHIP rises at a quick pace, activity tracker ownership has begun to plateau. *Wearables Authority*, 13 jul. 2015. Disponível em: <http://authoritywearables.com/smartwatch-ownership-rises-at-a-quick-pace-activity-tracker-ownership-has-begun-to-plateau>. Acesso em: 31 jan. 2017.

[140] THE INTERNET of things is actually full of useless things. *Next Big What*, 6 fev. 2015. Disponível em: <www.nextbigwhat.com/Internet-of-useless-things-297/>. Acesso em: 31 jan. 2017.

[141] CROUAN, Raph. Corporates must help stop us creating an Internet of useless things. *New Statesman*, jun. 2016. Disponível em: <http://tech.newstatesman.com/iot/Internet-useless-things>. Acesso em: 31 jan. 2017.

[142] Sobre o tema, vide ROMAN, Rodrigo; ZHOU, Jianying; LOPEZ, Javier. On the features and challenges of security and privacy in distributed Internet of things. *Computer Networks*, n. 57. p. 2266-2279, 2013; WEBER, Rolf H. Internet of things: new security and privacy challenges. *Computer Law & Security Review*, n. 26. p. 23-30, 2010.

indivíduos em seus hábitos, preferências, desejos e tentando, assim, direcionar suas escolhas.

Tal necessidade foi bem enxergada pelo mercado, que tem explorado a possibilidade de personalização e customização automática de conteúdo nas plataformas digitais, inclusive capitalizando essa filtragem com publicidade direcionada por meio de rastreamento de *cookies* e processos de *retargeting* ou mídia programática (*behavioral retargeting*)[143].[144]

A *Federal Trade Commission* dos Estados Unidos demonstrou preocupações com a segurança do ecossistema de IoT.[145] Por conta disso, questionou o *Department of Commerce* recentemente sobre o assunto.[146] A *Federal Trade Commission* estima que cerca de 10.000 habitantes podem gerar 150 milhões de *data points*[147] diariamente.[148] Os dispositivos captam as informações, enviam para a central e depois compilam os dados de acordo com as preferências do usuário.[149]

Não se tem, hoje, clareza do tratamento despendido aos dados.[150] Aspectos sobre a coleta, o compartilhamento e o potencial uso deles por terceiros ainda são

[143] MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.
[144] OLIVEIRA, Márcio. Em marketing, Big Data não é sobre dados, é sobre pessoas! *Exame*, out. 2016. Disponível em: <http://exame.abril.com.br/blog/relacionamento-antes-do-marketing/em-marketing-bigdata-nao-e-sobre-dados-e-sobre-pessoas/>. Acesso em: 31 jan. 2017.
[145] FTC Staff Report. "Internet of things: privacy & security in a connected world", 2015, op. cit.
[146] FISHER, Dennis. The Internet of dumb things. *Digital Guardian*, 13 out. 2016b. Disponível em: <https://digitalguardian.com/blog/Internet-dumb-things>. Acesso em: 1 fev. 2017; FISHER, Dennis. FTC warns of security and privacy risks in IoT devices. *On The Wire*, 3 jun. 2016a. Disponível em: <www.onthewire.io/ftc-warns-of-security-and-privacy-risks-in-iot-devices/>. Acesso em: 31 jan. 2017.
[147] "Um *data point* é uma unidade discreta de informações. Em um sentido geral, qualquer fato é um *data point*. Em um contexto estatístico ou analítico, um ponto de dados geralmente é derivado de uma medida ou pesquisa e pode ser representado numericamente e/ou graficamente. O termo é equivalente a *datum*, a forma singular de dados." Definição disponível em: <http://whatis.techtarget.com/definition/data-point>. Acesso em: 10 out. 2017. (Lê-se no original "*A data point is a discrete unit of information. In a general sense, any single fact is a data point. In a statistical or analytical context, a data point is usually derived from a measurement or research and can be represented numerically and/or graphically. The term data point is roughly equivalent to datum, the singular form of data*").
[148] FTC Staff Report. "Internet of things: privacy & security in a connected world", 2015, op. cit.
[149] FISHER, Dennis. "The Internet of dumb things", 2016b, op. cit.
[150] ACCENTURE. *Digital trust in the IoT era*, [s.d.]. Disponível em: <www.accenture.com/t20160318T035041__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-3-Digital-Trust-IoT-Era.pdf>. Acesso em: 31 jan. 2017.

desconhecidos pelos consumidores. Isso tem competência para abalar – e, em certo sentido, já abala –[151] a confiança dos usuários nos produtos conectados.[152]

Salienta-se, ainda, o fato de que as falhas de segurança abrem espaço para ataques visando ao acesso às informações geradas pelos próprios dispositivos. Além disso, os aparelhos inteligentes, quando invadidos, podem gerar problemas não só para o aparelho em si, interferindo também na própria infraestrutura da rede. Foi o que aconteceu no final de 2016 com o ataque DDoS[153],[154] ocasião na qual *hackers* conseguiram suspender diversos *sites* invadindo os servidores por meio de câmeras de segurança, revelando a vulnerabilidade desses dispositivos. Portanto, questões relacionadas à segurança e proteção de dados pessoais são igualmente importantes para que a IoT se consolide como o próximo passo da Internet.

O aumento da oferta de produtos "inúteis" pode enfraquecer todo o mercado de IoT. Por vezes, convincentes estratégias de marketing fazem com que as pessoas adquiram objetos que sequer lhes serão úteis ou que se mostravam úteis à primeira vista, mas que, com o uso, revelaram sua inutilidade. Muitos objetos apenas combinam funcionalidades em um espaço muito pequeno, como é o caso hoje dos *smart watches*, sacrificando a usabilidade só pela novidade. Essa técnica publicitária massiva que convence o consumidor a adquirir os mais

[151] BOLTON, David. 100% of reported vulnerabilities in the Internet of Things are Avoidable. *Applause*, set. 2016. Disponível em: <https://arc.applause.com/2016/09/12/Internet-of-things-security-privacy/>. Acesso em: 31 jan. 2017; CONSUMER TECHNOLOGY ASSOCIATION. *Internet of things*: a framework for the next administration (white paper), 2016. Disponível em: <www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf>. Acesso em: 31 jan. 2017; ACCENTURE. "Digital trust in the IoT era", [s.d.], op.cit.; PLOUFFE, James. The ghost of IoT yet to come: the Internet of (insecure) things in 2017. *Mobile Iron*, 23 dez. 2016. Disponível em: <www.mobileiron.com/en/smartwork-blog/ghost-iot-yet-come-Internet-insecure-things-2017>. Acesso em: 31 jan. 2017.

[152] MEOLA, Andrew. How the Internet of things will affect security & privacy. *Business Insider*, 19 dez. 2016. Disponível em: <www.businessinsider.com/Internet-of-things-security-privacy-2016-8>. Acesso em: 31 jan. 2017.

[153] Ataque DDoS, um acrônimo em inglês para Distributed Denial of Service ou, em português, ataque distribuído de negação de serviço, é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores através de uma sobrecarga produzida por máquinas zumbis, entre outros métodos.

[154] COBB, Stephen. 10 things to know about the october 21 DDoS attacks. *We Live Security*, 24 out. 2016. Disponível em: <www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/>. Acesso em: 31 jan. 2017.

diversos objetos, acaba, segundo alguns autores, nos transformando em escravos da tecnologia.[155]

Não se pretende, com isso, tecer críticas absolutas à inovação tecnológica, que proporciona inegáveis benefícios à sociedade. Nada obstante, muitas vezes a inovação é guiada unicamente por fins mercadológicos, de modo que, desde que as criações sejam rentáveis, não importa se terão real utilidade. Basta que os consumidores pensem que elas a possuem.

Como bem pontuou Jenny Judge:[156]

> Mas mesmo que as empresas de tecnologia não estejam realmente tentando nos escravizar ou nos fazer sentir inadequados, isso não significa que a situação atual seja um caso de boas intenções que deram errado. Não há maior razão para pensar que a tecnologia é intrinsecamente boa, mas ocasionalmente dá errado, do que há para pensar que ela é um vilão extremamente bem-sucedido.
> (...)
> Nós amamos elogiar a tecnologia, e nós amamos condená-la. Nós a equiparamos ao caos, ao poder, ao amor, ao ódio; à democracia, à tirania, ao progresso e à regressão – nós a louvamos como nossa salvação, enquanto a lamentamos como nosso flagelo. Como qualquer tecnologia que veio anteriormente, a tecnologia digital é tudo isso. Mas não é essencialmente nada disso. [157]

Há casos de criações voltadas ao mercado de IoT que não atendem a uma necessidade da sociedade nem geram um aprimoramento tecnológico significativo e tampouco são guiados exclusivamente por uma demanda do mercado. Ainda assim, muitas dessas criações conseguem proteção por propriedade intelectual, consideradas como invenções. Vamos problematizar brevemente o enquadramento dessas criações como invenções tecnológicas protegidas por lei.

Considera-se uma invenção a criação intelectual de efeito técnico ou industrial.[158] Portanto, para que seja considerada uma invenção *stricto sensu*, não

---

[155] JUDGE, Jenny. Are we liberated by tech - or does it enslave us? *The Guardian*, 9 dez. 2015. Disponível em: <www.theguardian.com/technology/2015/dec/09/are-we-liberated-by-tech-or-does-it-enslave-us>. Acesso em: 26 jan. 2017.

[156] Ibid.

[157] Tradução livre do autor. No original: "*But even if tech companies aren't really trying to enslave us, or to make us feel inadequate, that doesn't mean that the current situation is a case of good intentions gone awry. There's no more reason to think that tech is intrinsically good, but occasionally getting it wrong, than there is to think that it's a remarkably successful villain.*
We love to praise tech, and we love to condemn it. We equate it with chaos, power, love, hate; with democracy, with tyranny, with progress and regress - we laud it as our salvation, while lamenting it as our scourge. Like any technology that has come before it, digital technology is all of these things. But it's essentially none of them".

[158] Na conceituação de João da Gama Cerqueira, "A invenção, pela sua origem, caracteriza-se como uma criação intelectual, como o resultado da atividade inventiva do espírito humano; pelo modo de sua realização, classifica-se como uma criação de ordem técnica; e, pelos seus fins,

basta ser uma criação do intelecto; é necessário que haja uma solução nova para um problema técnico existente.[159]

O título jurídico pelo qual se protege uma invenção, assegurando ao seu titular uma relação de domínio ou propriedade,[160] denomina-se patente. Confira-se o que leciona Alexandra Godoy Corrêa:

> A patente de invenção, além de proteger a invenção, é um título expedido pelo Estado, através do órgão competente para tanto – no Brasil, o Instituto Nacional da Propriedade Industrial (Inpi) – que outorga ao seu titular a propriedade e exclusividade de exploração da invenção, por período limitado.[161]

Para que uma patente seja concedida, o legislador pátrio enumerou, expressamente, três requisitos que caracterizam a invenção, todos devendo estar presentes de forma independente e cumulativa, como se observa pelo disposto no art. 8º da Lei nº 9.279/1996: "Art. 8º. É patenteável a invenção que atenda aos requisitos de novidade, atividade inventiva e aplicação industrial".[162]

Nem toda invenção é considerada nova[163] – mesmo que para seu mentor o seja – por já poder estar acessível ao público. Ainda que se trate de novidade por

---

constitui um meio de satisfazer às exigências e necessidades práticas do homem" (CERQUEIRA, João da Gama. *Tratado de propriedade industrial*. 2. ed. São Paulo: RT, 1982. v. I).

[159] CORRÊA, Alexandra Barbosa de Godoy. Patentes de medicamentos e o princípio da função social da propriedade no Brasil. *Revista Propiedad Intelectual*, Mérida, ano XIII, n. 17, p. 63, jan./dez. 2014.

[160] Para Gama Cerqueira, "A patente de invenção, expedida pela administração pública, mediante o cumprimento das formalidades legais e sob certas condições, é o ato pelo qual o Estado reconhece o direito do inventor, assegurando-lhe a propriedade e o uso exclusivo da invenção pelo prazo da lei. É o título do direito de propriedade do inventor. Constitui, ao mesmo tempo, a prova do direito e o título legal para o seu exercício. Em sentido figurado significa o próprio privilégio" (CERQUEIRA, João da Gama. *Tratado de propriedade industrial*, 1982, op. cit., p. 202). Confira, ainda, a definição de MACEDO, Maria Fernanda Gonçalves; BARBOSA, A. L. Figueira. *Patentes, pesquisa & desenvolvimento*: um manual de propriedade industrial. Rio de Janeiro: Fiocruz, 2000, p. 23: "A invenção pode ser descrita como uma nova solução para um problema técnico de produção. O problema pode ser antigo ou novo; respectivamente, de como criar ou aperfeiçoar um processo químico ou um novo produto para atender a uma necessidade antes inexistente. Mas a solução, para ser uma invenção, precisa ser obrigatoriamente nova, ou seja, que ninguém haja criado anteriormente a ideia ou, pelo menos, que ninguém tenha divulgado ou disponibilizado o acesso de sua informação ao público".

[161] CORRÊA, Alexandra Barbosa de Godoy. "Patentes de medicamentos e o princípio da função social da propriedade no Brasil", 2014, op. cit., p. 64.

[162] Cf. MAGRANI, Bruno et al. *Direitos intelectuais*, 2014. Disponível em: <https://direitorio.fgv.br/sites/direitorio.fgv.br/files/u100/direitos_intelectuais_2014-2.pdf>. Acesso em: 29 mar. 2017.

[163] Sobre o conceito de novidade, veja-se PHILPOTT, Jeremy. Patents. In: ____; JOLLY, Adam. (Ed.). *A handbook of intellectual property management*: protecting, developing and exploiting your IP assets. Londres: The Patent Office/BTG, 2004, p. 162: "*The invention must not previously be known in the public domain anywhere in the world prior to the filing date of the patent application. If someone else has previously invented the same or similar technology, and disclosed it, the patent application will fail*".

não ter sido requisitado o pedido de registro de uma mesma invenção em nenhum outro país, a invenção ainda poderá não se encaixar nos requisitos da atividade inventiva caso seja uma criação evidente ou óbvia, para um técnico no assunto, consistindo esse no segundo requisito e, portanto, não permitindo que a criação seja patenteável. Assim, a condição de patenteabilidade referente à atividade inventiva deve ser analisada a partir dos conhecimentos de um técnico no assunto e não de uma pessoa qualquer.[164]

O terceiro requisito de fundo da patenteabilidade de uma invenção é a aplicação industrial, disposta no art. 15 da Lei nº 9.279/1996. Caso o uso na indústria ou a fabricação da invenção seja possível, estará preenchido o requisito da aplicação industrial.[165]

Entretanto, para o cumprimento desses requisitos, a maior dificuldade que se encontra é a própria definição da utilidade ou caráter industrial da invenção,[166] tendo em vista a completa falta de critérios para uma apreciação adequada e suficiente.

Para Denis Borges Barbosa, utilidade industrial significa "que a tecnologia seja capaz de emprego, modificando diretamente a natureza, numa atividade econômica qualquer".[167] Já Nathan Machin, apresentando a controvérsia sobre a conceituação de utilidade no direito norte-americano, pontua que a Suprema Corte já apresentou diferentes definições, destacando-se dois requisitos básicos: (1) a *utilidade específica* requer que a invenção funcione e (2) a *utilidade geral* requer que a invenção seja direcionada a um desejo ou a uma necessidade humana. Além dessas definições (utilidades específica e geral), o autor apresenta outras duas: a *utilidade prática*, que exige que a invenção com fins terapêuticos atenda a determinados padrões elevados, e a *utilidade moral*, que requer que as invenções

---

[164] MAGRANI, Bruno et al. "*Direitos intelectuais*", 2014, op. cit.
[165] Ibid.
[166] PHILPOTT, Jeremy. "Patents", 2004, op. cit. p. 163: "*The invention must have a use, even if it is only a toy or game. No patent office requires working models, nor does any have laboratories where they verify the claims of patent applicants about the efficacy of their inventions. The patent examiners have to take the applicant's experimental data at face value. However, those inventions that manifestly do not work (such as perpetual motion machines) are refused patent protection. The requirement that an invention has a use excludes pure discoveries from patent protection. This means that the discovery of penicillin (a naturally occurring substance) was not itself patentable, although patents were granted when it was worked up into a shelf-stable form for use as an antibiotic (namely a useful application for the discovery, rather than for the discovery itself)*".
[167] BARBOSA, Denis Borges. Uma introdução à propriedade industrial. 2. ed. rev. e atual. Rio de Janeiro: Lumen Juris, 2003. p. 319.

não sejam nocivas. Nathan Machin propõe a doutrina da utilidade prospectiva, que seria aplicável a todas as invenções, como uma fórmula de determinar a utilidade. Três seriam as principais distinções desta doutrina: (1) ela define utilidade como promotora do progresso das artes úteis; (2) permite que alguém estabeleça utilidade ao demonstrar que uma pessoa de habilidades ordinárias na arte acreditaria, de forma razoável, que a invenção tem chances razoáveis de ter usos significativos no futuro; (3) permite que o candidato à patente apresente evidências de sucessos comerciais como evidência da utilidade.[168]

Vale, ainda, conferir os ensinamentos de Bercovitz,[169] para quem "a invenção, para ser considerada invenção industrial, deve pertencer ao campo da indústria, entendida esta como a atividade que persegue por meio de uma atuação consciente dos homens, fazer útil as forças naturais para a satisfação das necessidades humanas".[170-171]

A conceituação de utilidade é de importância capital para o estudo da patenteabilidade de dispositivos da IoT, uma vez que uma análise descuidada pode levar à proteção e ao monopólio de exploração de objetos que não possuem real utilidade.[172] Diversas criações relacionadas à IoT conseguiram conquistar a proteção intelectual como invenções por conta de um julgamento leviano do órgão responsável pelo registro.

Como afirma Raph Crouan, a IoT é uma palavra da moda, mas é preciso que as empresas atuem de modo conjunto para criar soluções para problemas atuais. Do contrário, há o risco de que a IoT se concentre na Internet das coisas

---

[168] MACHIN, Nathan. Prospective utility: a new interpretation of the utility requirement of section 101 of the Patent Act. *California Law Review*, v. 87, n. 2, p. 423-436, 1999.
[169] MAGRANI, Bruno et al. "Direitos intelectuais", 2014, op. cit.
[170] Cf. BERCOVITZ, A. Los requisitos positivos de patenteabilidad en el derecho alemán, Madri, 1969, p. 446 apud BERGEL, Salvador D. Requisitos y excepciones a la patenteabilidad: invenciones biotecnológicas. In: CORREA, Carlos M. (Coord.). *Derecho de patentes, el nuevo regimen legal de las invenciones y los modelos de utilidad*. Buenos Aires: Ciudad Argentina, 1996. p. 23.
[171] MAGRANI, Bruno et al. "Direitos intelectuais", 2014, op. cit.
[172] A tecnologia digital não necessariamente torna a vida das pessoas mais fácil e os custos para conectar um dispositivo são altos e os benefícios talvez sejam baixos demais para compensar o aumento de valor no produto. Muitas vezes, uma tecnologia de IoT como o *EggMinder (bandeja com sensor que informa quantos ovos existem na geladeira)*, acabaria sendo um dispositivo caro, com configurações complexas e baterias que precisam ser recarregadas constantemente. Isto não parece tão inteligente. Vide: https://medium.com/@eduardomagrani/seja-bem-vindo-%C3%A0-internet-das-coisas-in%C3%BAteis-878781af0bf4.

inúteis.[173] O Estado, por meio do órgão responsável pelo registro de patentes, deve estar atento ao cumprimento dos requisitos patentários, visto que a concessão do monopólio de exclusividade sobre uma criação intelectual deve visar também à função social dessa criação, e, para tanto, esta deve atender a uma necessidade da sociedade.

Nesse sentido, segundo a pesquisadora em direito e política tecnológica da Universidade de Cambridge, Julia Powles, é necessário pensarmos em desenvolver uma "Internet das pessoas" e não somente das coisas. Segundo Powles, a IoT pode ser usada como desculpa para o consumismo desenfreado, cuja única contribuição será "lotar nossos porões com tranqueiras desnecessárias". [174] Além disso, no pior cenário, ficaríamos sob constante vigilância por conta dos objetos que adquirimos.[175][176]

Diante desse cenário, Samuel Greengard pontua que há um grupo muito otimista quanto à IoT, mas há outro que não vê as coisas de forma tão positiva, afirmando que a IoT pode descortinar um futuro distópico semelhante ao descrito por George Orwell em 1984.

O autor bem sintetiza a questão:[177]

> Na realidade, a IoT irá provavelmente pousar em algum ponto entre as duas extremidades do espectro. Ela vai introduzir muitos dispositivos frívolos e inúteis que desaparecem rapidamente, mas também oferecem sistemas altamente práticos e soluções que melhoram a qualidade de vida. Isso tornará as coisas mais fáceis e seguras de algumas maneiras, mas mais difíceis e desafiadoras em outras. [...] Só o tempo revelará eventualmente essas respostas e nos deixará saber se um mundo conectado realmente é igual a um mundo melhor.[178]

---

[173] CROUAN, Raph. "Corporates must help stop us creating an Internet of useless things", 2016, op. cit.
[174] POWLES, Julia; JUDGE, Jenny. Internet das coisas ou das pessoas? Trad. Rafael A. F. Zanatta. *Outras Palavras*, 27 maio 2016. Disponível em: <http://outraspalavras.net/posts/377086/>. Acesso em: 31 jan. 2017.
[175] Ibid.
[176] KARASINSKI, Lucas. "O que é tecnologia?", 2013, op. cit.
[177] GREENGARD, Samuel. *The Internet of things*. Cambridge, MA: The MIT Press, 2015. p. 188-189.
[178] Tradução livre do autor. No original: "*In reality, the IoT will likely land somewhere between the two ends of the spectrum. It will introduce plenty of frivolous and useless devices that quickly disappear but also deliver highly practical systems and solutions that improve the quality of life. It will make things easier and safer in some ways but more difficult and challenging in others. […] Only time will eventually reveal these answers and let us know if a connected world really equals a better world*".

Por outra perspectiva, as pesquisadoras Jenny Judge e Julia Powles destacam os lados negativos das invenções relacionadas à Internet das coisas:[179]

> Na melhor das hipóteses, a Internet das coisas é apenas mais uma desculpa para o consumismo desenfreado, cuja única contribuição será a de obstruir os porões com mais lixo desnecessário. Mas, na pior das hipóteses, objetos domésticos diários serão transformados em espiões inimigos, colocando-nos sob vigilância constante. Seremos cutucados e manipulados a cada momento. Nossas vidas e posses serão perpetuamente expostas a hackers. A Internet das coisas de fato irá encher nossas casas com objetos, mas esses objetos estão longe de serem encantados – eles são amaldiçoados.[180]

As autoras afirmam, ainda, que devemos unir os mundos físico e digital, de modo que tenhamos controle de nossas informações e que a tecnologia seja usada de forma inteligente. Confira-se:[181]

> A saída é contraintuitiva. Em suma, precisamos nos esquecer das coisas. Precisamos parar de nos obcecar com objetos "inteligentes" e começar a pensar com inteligência sobre as pessoas. Nós dificilmente podemos desviar nosso olhar de nossos portais para a Internet. E esses dispositivos estão entrando no nosso caminho. Estarmos acorrentados a nossas mesas está cortando pedaços de nossas vidas. Olhar fixamente para nossos smartphones está prejudicando nossas colunas. Estamos perdendo o sono. Nossa visão está falhando. Nossas próprias identidades estão ameaçadas pela rede opaca. *Algo deve mudar*. [...] Este é o verdadeiro potencial da Internet das coisas. Poderia colocar nossos vastos armazéns de conhecimento tácito e corpóreo para trabalhar online. Poderia unir os mundos físico e digital. E poderia colocar-nos no controle da nossa própria informação e integridade contextual, num contexto moral e político *compromissado, de forma resoluta*, com os direitos humanos, o Estado de direito e a coesão social. Poderia se tornar uma Internet não de coisas inteligentes, mas de pessoas inteligentes e capacitadas. [...] A Internet tornou-se uma parte tão onipresente de nossas vidas que tendemos a esquecer que ela está em sua infância. Ainda é apenas um protótipo bruto do que poderia ser. A Internet do futuro não precisa ser como a Internet de hoje: plana, monopolizada e perigosamente opaca. Sua forma, contornos e sensação ainda estão, literalmente, em disputa.[182]

---

[179] JUDGE, Jenny; POWLES, Julia. Forget the Internet of things: we need an Internet of people. *The Guardian*, 25 maio 2015. Disponível em: <www.theguardian.com/technology/2015/may/25/forget-Internet-of-things-people>. Acesso em: 30 jan. 2017.

[180] Tradução livre do autor. No original: "*at best, the Internet of things is just another excuse for rampant consumerism, whose only contribution will be to clog basements with yet more unnecessary junk. But at worst, everyday household objects will be turned into enemy spies, placing us under constant surveillance. We will be nudged and manipulated at every moment. Our lives and possessions will be perpetually exposed to hackers. The Internet of things will fill our homes with objects all right, but those objects are far from enchanted – they are cursed*".

[181] JUDGE, Jenny; POWLES, Julia. "Forget the Internet of things: we need an Internet of people", 2015, op. cit, grifos do autor.

[182] Tradução livre do autor. No original: "*The way out is counterintuitive. In short, we need to forget about the things. We need to stop obsessing over "smart" objects, and start thinking smart*

Vale ressaltar, neste ponto, a opinião de Sérgio Czajkowski Jr., professor da Universidade Positivo e do UniCuritiba, segundo o qual "mesmo sendo inegável que a tecnologia foi vital para uma 'evolução' da humanidade, é salutar sempre se mencionar que esta não é neutra e que nem todos os avanços tecnológicos redundaram em benefícios para toda a humanidade".[183]

Sobre esse aspecto, vale citar Estéfano Veraszto que examina em seu estudo[184] "Tecnologia: Buscando uma definição para o conceito" as diferentes concepções e correntes acerca da tecnologia.[185] O autor explica no bojo deste

---

about people. We can hardly tear our gaze away from our portals to the Internet. And these devices are getting in our way. Being chained to our desks is lopping chunks off our lifespans. Staring at our smartphones is damaging our spines. We're losing sleep. Our eyesight is failing. Our very identities are threatened by the opaque web. Something must change […]. This is the true potential of the Internet of things. It could put our vast stores of tacit, embodied knowledge to work online. It could unite the physical and digital worlds. And it could put us in control of our own information and contextual integrity, against a moral and political backdrop that is resolutely committed to human rights, the rule of law and social cohesion. It could become an Internet, not of smart things, but of smart, empowered people. […]. The Internet has become such an ubiquitous part of our lives that we tend to forget that it is in its infancy. It's still just a crude prototype of what it could be. The Internet of the future doesn't have to be like the Internet of today: flat, monopolised and dangerously opaque. Its form, contours and feel are still, quite literally, up for grabs".

[183] Cf. Sérgio Czajkowski Jr. apud KARASINSKI, Lucas. "O que é tecnologia?", 2013, op. cit.

[184] VERASZTO, Estéfano Vizconde et al. Tecnologia: Buscando uma definição para o conceito. PRISMA.COM, n. 7, p. 60-85, 2008. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/viewFile/681/pdf>. Acesso em: 02 mai. 2017.

[185] Tratando de outras correntes além da neutralidade tecnológica, Estéfano Veraszto examina, após, a concepção do determinismo tecnológico. Segundo o autor, esta concepção considera a tecnologia "como sendo autônoma, auto-evolutiva, seguindo, de forma natural, sua própria inércia e lógica de evolução, desprovida do controle dos seres humanos. A imagem da tecnologia autônoma e fora do controle humano, desenvolvendo-se segundo lógica própria, aparece associada a uma concepção determinista das relações entre tecnologia e sociedade. Segundo essa corrente, portanto, o progresso tecnológico segue um caminho fixo e, mesmo que fatores políticos, econômicos ou sociais possam exercer alguma influência, não se pode alterar o poderoso domínio que a tecnologia impõe às transformações sociais. Para Veraszto, "afirmar isso é descontextualizar a tecnologia e ignorar as redes de interesses sociais decisivos para a escolha de uma ou outra tecnologia. Sem dúvida, o desenvolvimento tecnológico terá um impacto social, poderá alterar nossos padrões de vida e convivência chegando a gerar outros totalmente distintos, mas esse desenvolvimento é sustentado por uma série de interesses e valores externos e não age por lógica própria. (...) Prever todas as conseqüências que uma determinada tecnologia pode trazer é tão difícil como prever todos os rumos evolutivos que uma sociedade pode tomar. Essa tese de autonomia tecnológica impede uma análise crítica do processo tecnológico, pois libera engenheiros, cientistas e políticos de suas responsabilidades, abrindo caminho para o irracionalismo romântico ou para a tecnocracia medíocre". Outra corrente explicada pelo autor diz respeito à concepção de universalidade da tecnologia segundo a qual "o caráter universal das leis científicas leva a uma concepção de que a tecnologia não requer uma contextualização social, nem tampouco devem ser levados em consideração os caracteres valorativos, tendo em vista que a tecnologia, como sendo fruto do desenvolvimento científico, é neutra. Assim, podemos dizer que essa concepção aponta que os resultados obtidos do desenvolvimento tecnológico são válidos independemente do contexto cultural, político, social ou econômico do local onde foi gerado. Isso dá a idéia que mesma tecnologia não tem seu uso modificado se inserida em outro contexto". O

estudo a concepção de neutralidade da tecnologia, segundo a qual "a tecnologia não é boa nem má. Seu uso é que pode ser inadequado. Seria o mesmo que dizer que a tecnologia está isenta de qualquer tipo de interesse particular tanto em sua concepção e desenvolvimento como nos resultados finais".

O autor faz, no entanto, uma crítica a essa corrente:[186]

> Sabemos que a tecnologia não é neutra; um artefato aparentemente inócuo pode estar carregado de interesses políticos (e/ou outros) A tecnologia, longe de ser neutra, reflete os planos, propósitos e valores da nossa sociedade. Fazer tecnologia é, sem dúvida, fazer política e, dado que a política é um assunto de interesse geral, deveríamos ter a oportunidade de decidir que tipo de tecnologia desejamos. Mantendo o discurso que a tecnologia é neutra favorece a intervenção de experts que decidem o que é correto baseando-se em uma avaliação objetiva e impede, por sua vez, a participação democrática na discussão sobre planejamento e inovação tecnológica.
> (...)
> Tanto as técnicas como as tecnologias abrangem de maneira indissolúvel, interações entre pessoas vivas e pensantes, entre entidades materiais e artificiais e, ainda, entre idéias e representações. Cada sociedade cria, recria, pensa, repensa, deseja e age sobre o mundo através da tecnologia e de outros sistemas simbólicos. A tecnologia é impensável sem admitir a relação entre o homem e a sociedade. O desenvolvimento de novas tecnologias, sejam elas produtos, artefatos ou sistemas de informação e comunicação, constitui um dos fatores chave para compreender e explicar todas as transformações que se processam em nossa sociedade. E, desta maneira, podemos dizer que a tecnologia está intrinsecamente associada aos valores humanos. (...) A tecnologia abrange um conjunto organizado e sistematizado de diferentes conhecimentos, científicos, empíricos e intuitivos. Sendo assim, possibilita a reconstrução constante do espaço das relações humanas. (...) A tecnologia, uma vez colocada à disposição da sociedade ou do mercado, passa a ter seu valor determinado pela forma como vai ser adquirida e usada, e quem define esse valor (de bem ou de consumo) é a própria sociedade em desenvolvimento. Sendo o desenvolvimento um elemento dentro de uma cultura, a tecnologia se torna produto da sociedade que a cria.

---

autor trata ainda das correntes pessimistas e otimistas acerca da tecnologia. No viés pessimista, em explicação do autor, "Segundo o filósofo alemão Martin Heidegger a técnica é um fenômeno tipicamente moderno, responsável por um progresso tecnológico que é a causa de todos os males da humanidade, por contribuir para alargar as desigualdades sociais, graças ao acúmulo discrepante de riquezas e poder. Quem defende esse ponto de vista, afirma que a tendência é piorar sempre. Mesmo sabendo que Heidegger se referiu à tecnica podemos transpor esse ponto de vista para a tecnologia. E utilizando essa visão como norte, muitas pessoas hoje acreditam, ou defendem a tese, de que o progresso tecnológico é e será responsável pela extinção da vida na Terra e/ou a destruição do planeta". Já o viés otimista, segundo Veraszto, enxerga "a tecnologia como uma forma de garantir o progresso e o bem estar social". VERASZTO, Estéfano Vizconde et al. Tecnologia: buscando uma definição para o conceito. *Prisma.com*, n. 7, p. 60-85, 2008. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/viewFile/681/pdf>. Acesso em: 2 maio 2017.

[186] VERASZTO, Estéfano Vizconde et al. *Tecnologia:* Buscando uma definição para o conceito. PRISMA.COM, n. 7, p. 60-85, 2008. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/viewFile/681/pdf>. Acesso em: 02 mai. 2017.

O renomado filósofo italiano Umberto Galimberti em sua tese sobre "o humano na idade da técnica" sustenta que as técnicas e as tecnologias são de fato a nossa própria natureza, já que as fazemos, dia após dia, mas, de igual maneira, elas também nos fazem, num só movimento de reciprocidade.[187] Segundo Galimberti:[188]

> Pensar as técnicas e tecnologias como problema não é tarefa fácil. Estamos tão acostumados a concebê-las preponderantemente como solução, que é bastante improvável que, em termos de reflexão, consigamos percebê-las (também) como um possível problema. As técnicas e tecnologias nos oferecem solução e alívio para uma série de atividades e problemas que, de outra maneira, seriam impossíveis de serem realizados, ou que teríamos de resolver por nossa própria conta, sem o auxílio de máquinas, instrumentos e ferramentas, ou seja, algo até improvável. Foi por meio de nossa história trilhada tecnicamente que construímos nossas sociedades, nossas cidades, e foi assim também que acabamos nos transformando no filo mais predominante do planeta. Nós concebemos e utilizamos as técnicas e tecnologias, estruturamo-nos socioculturalmente e compreendemos o mundo por meio delas – sustentamos –, mas acabamos igualmente sendo determinados por seus próprios determinismos. (...) A técnica, comumente considerada uma ferramenta à disposição do homem, tornou-se, hoje, o verdadeiro "sujeito" da História.

Com todos esses exemplos, mesmo que a Internet esteja sendo levada às Coisas, estas estão conectadas a nós, as pessoas a quem essas coisas passarão a prover serviços e funcionalidades. É nesse sentido que devemos compreender que estamos falando sempre de uma Internet das pessoas. Devemos evoluir também na análise crítica a respeito da utilidade dessas criações e nas questões de privacidade e de segurança que elas geram.

Pretende-se, com isso, dar os incentivos (sociais e estatais) corretos para que os benefícios sejam sempre maiores do que qualquer malefício decorrente dessa conectividade. Devemos refletir ainda sobre os impactos desses produtos sobre nosso comportamento. Tudo isso é incorporado à nossa rotina de forma imperceptível, mas causa, rapidamente, uma alta dependência pelo conforto e pela comodidade que essa nova realidade nos traz. Devemos nos preocupar em como a ampliação da nossa conexão com as "coisas" será capaz de gerar efeitos positivos na sociedade, melhorando nosso bem-estar, nossos relacionamentos interpessoais e atendendo a requisitos de utilidade e função social.

---

[187] Disponível em: http://filosofia.uol.com.br/o-humano-na-idade-da-tecnica/. Acesso em: 28 mar. 2017.
[188] GALIMBERTI, Umberto. *The human being in the age of technique Unisinos*. 2015.

Para entendermos melhor o surgimento do conceito de IoT e buscarmos compreender a razão pela qual ela vem sendo associada ao conceito de web 3.0, possuindo em suas manifestações um forte componente de tecnologia inovadora, iremos analisar as diferentes fases por meio das quais a rede vem se modificando e aprimorando, até a chegada desse novo conceito.[189]

1.1
Origem e Taxonomia da Iot: as três eras da Internet

O conceito da IoT está relacionado a uma nova era da Internet, chamada de Web 3.0, mas antes de chegarmos ao cenário atual, muitas conceituações e evoluções ocorreram e serão resumidamente explicadas a seguir.

A Internet[190] surgiu no final da década de 1960, criada no bojo do projeto ARPANET [191] (Advanced Research Projects Agency Network) vinculado à Agência DARPA (Defense Advanced Research Projects Agency)[192], financiado pelo governo federal dos Estados Unidos com o intuito de construir uma comunicação resistente a falhas ou ataques locais, por meio da criação de uma rede de computadores interconectados, utilizando o protocolo TCP/IP para comunicar entre si.[193]

[189] As invenções relacionadas à Internet das coisas passam a interagir entre elas e com as pessoas, geralmente por meio de três etapas: (1) identificação: "o sistema precisa registrar os dados de cada aparelho" e conectar esses objetos a bases de dados e à Internet; (2) sensores: "o sistema detecta mudanças na qualidade física dos objetos"; (3) "miniaturização e nanotecnologia: pequenos objetos com a capacidade de interagir e se conectar a [*sic*] grande rede" (GIELFI, Marcella. "Internet das coisas" x "Internet de tudo": como isso vai mudar seu cotidiano em breve. *Ideia de Marketing,* 22 abr. 2013. Disponível em: <www.ideiademarketing.com.br/2013/04/22/Internet-das-coisas-x-Internet-de-tudo-como-isso-vai-mudar-seu-cotidiano-em-breve/>. Acesso em: 8 maio 2017.

[190] O que chamamos hoje comumente de "Internet" consiste em um conjunto de computadores conectados entre si por meio de várias redes que se conectam uma à outra até formar a grande rede ou Internet, utilizando o protocolo TCP/IP para comunicar entre si.

[191] Disponível em: <https://pt.wikipedia.org/wiki/ARPANET>. Acesso em: 03 out. 2017.

[192] Há certa confusão terminológica na doutrina: enquanto alguns autores utilizam a abreviação ARPA, outros se valem da DARPA. Como pontua Paul Ceruzzi, a ARPA (*Advanced Research Projects Agency*) foi fundada em 1958 e, posteriormente, foi renomeada, passando a se chamar *Defense Advanced Research Projects Agency*, cujo acrônimo é DARPA. O nome foi revertido para ARPA novamente em 1993. Alguns anos depois, o termo voltou a ser DARPA e é utilizado até hoje. Cf. o sítio eletrônico da DARPA: <https://www.darpa.mil/>. Acesso em: 28 jul. 2017 e CERUZZI, Paul E. The Internet before Commercialization. In: _____; ASPRAY, William (eds.). *The Internet and American Business*. Cambridge (MA): The MIT Press, 2008, p. 38.

[193] Cf. ABBATE, Janet. *Inventing the Internet*. Massachusetts: Massachusetts Institute of Technology, 1999 e HAFNER, Katie; LYON, Matthew. *Where wizards stay up late*: the origins of the Internet. New York: Touchstone Edition, 1998.

A ARPANET, como projeto bélico[194], serviu no início para a interconexão de redes militares regionais. Com o desenvolvimento da tecnologia e a possibilidade de transferir, por meio da rede, diversos tipos de mensagens, como voz e imagens, criou-se a possibilidade da comunicação entre os nós da rede sem que fosse necessário haver centros de controle. A primeira rede de computadores (ARPANET) tinha seus quatro nós localizados na Universidade da Califórnia em Los Angeles, no Stanford Research Institute, na Universidade da Califórnia em Santa Bárbara e na Universidade de Utah, e entrou em funcionamento em 1969.[195] O governo permitia que centros de pesquisa que colaboravam com o Departamento de Defesa dos EUA tivessem acesso à rede para fins de estudos direcionados ao departamento. Com o tempo, os cientistas passaram a usá-la para fins próprios, gerando embaraços à separação entre pesquisa com fins militares e com fins pessoais[196]. Foram criados, então, dois centros específicos: um destinado a aplicações militares e outro, a fins científicos. A ARPANET continuou a se expandir, de forma que em 1972 contava com 37 nós e em 1983, com 562[197].

Na década de 1970, os primeiros protocolos surgiram, a começar pelo NCP (*network control protocol*). A partir daí os próprios usuários puderam desenvolver aplicações. Vint Cerf e Robert Kahn criaram o TCP, que posteriormente foi dividido em TCP e IP.[198] Isso possibilitou o endereçamento de pacotes individuais e a administração de serviços como controle de tráfego e recuperação de serviços de maneira mais estável. O DARPA, então, firmou três contratos com a Universidade de Stanford para a implementação do TCP/IP. Esse foi o início de um longo período de experimentação e amadurecimento dos conceitos e mecanismos da Internet.[199]

No início da década de 1980, com a consolidação do protocolo TCP/IP como meio de comunicação entre as diversas redes de computadores e com o início da comercialização dos primeiros computadores pessoais (ARPANET 8800, Apple I e II), houve o crescimento exponencial de utilização da Internet como

[194] Disponível em: <http://www.teleco.com.br/tutoriais/tutorialww1/pagina_3.asp>. Acesso em: 03 out. 2017
[195] Disponível em: <https://pt.wikipedia.org/wiki/ARPANET>. Acesso em: 03 out. 2017.
[196] CASTELLS, Manuel. *A sociedade em rede*. Volume I. 8. ed. rev. e ampl. Tradução de Roneide Venancio Majer. São Paulo: Paz e Terra, 2005, p. 82-83.
[197] Disponível em: <http://paginas.fe.up.pt/~mgi97018/historia.html>. Acesso em: 28 jul. 2017.
[198] CASTELLS, Manuel. *A sociedade em rede*. 2005, op.cit.
[199] Disponível em: <http://www.cos.ufrj.br/uploadfile/1430748034.pdf>. Acesso em: 07 jul. 2017.

ambiente digital tecnológico, permitindo a difusão de LANs, PCs e *workstations* nos anos que se seguiram.[200]

Pesquisadores como Vint Cerf sentiram a necessidade de criar instituições voltadas para a coordenação dos mecanismos que sustentariam a internet, cada uma responsável por uma parte da rede. Foram criadas então entidades como a Internet Society (ISOC),[201] a IETF (Internet Engineering Task Force),[202] o IEEE (Institute of Electrical and Electronics Engineers) [203] e o ICANN (Internet Corporation for Assigned Names and Number*s*).[204]

Outra importante mudança diz respeito aos nomes de domínio e à capacidade dos roteadores. Para resolver tais questões, o DNS (*domain name system*)[205], o IGP (*Internet gateway protocol*) e o EGP (*exterior gateway protocol*) foram criados.

Por volta de 1985, a Internet já estava estabilizada como uma comunidade de pesquisadores e desenvolvedores ao redor do mundo. O próximo avanço significativo veio por intermédio de Tim Berners-Lee, Robert Cailliau e demais pesquisadores do CERN (Conseil Européen pour la Recherche Nucléaire) responsáveis por criar, no final da década de 1980, um protocolo eficiente para distribuir informação: a *world wide web* (www. ou "web") [206]. O principal acesso à Internet hoje no mundo se dá por meio da "web" que acabou se tornando, usualmente, sinônimo da própria Internet, mas que não deve ser confundido com esta.

Web é um termo simplificado de *world wide web*, que consiste em apenas uma das várias ferramentas de acesso à Internet. A web usa a Internet, mas ela em si não é a Internet. É uma aplicação criada para permitir o compartilhamento de arquivos (HTML e outros), tendo o *browser* (navegadores como Internet Explorer,

[200] RIBEIRO, Lígia Maria. Algumas notas sobre a história da Internet, *Faculdade de Engenharia da Universidade do Porto*, abr. 1998. Disponível em: <http://paginas.fe.up.pt/~mgi97018/historia.html>. Acesso em: 28 jul. 2017.
[201] Disponível em: <https://www.internetsociety.org/internet/history-internet/>. Acesso em: 05 dez. 2017.
[202] Disponível em: <https://www.ietf.org/about/>. Acesso em: 05 dez. 2017 e Disponível em: <https://www.ripe.net/participate/internet-governance/internet-technical-community/ietf>. Acesso em: 05 dez. 2017.
[203] Disponível em: <https://www.ieee.org/about/ieee_history.html>. Acesso em: 05 dez. 2017.
[204] Disponível em: <https://www.icann.org/history>. Acesso em: 05 dez. 2012.
[205] CERUZZI, Paul E. The Internet before Commercialization. In: _____; ASPRAY, William (eds.). *The Internet and American Business*. Cambridge (MA): The MIT Press, 2008, p. 32-38.
[206] RYAN, Johnny. *A history of the Internet and the digital future*. London: Reaktion Books, 2010, p. 105 e ss.

Safari e Chrome) como ferramenta de acesso. A web usa o protocolo HTTP para promover a transferência de informações e depende dos *browsers* para apresentar tudo isso ao internauta, permitindo que ele clique em *links* que levam a arquivos hospedados em outros computadores. A web é composta por: (1) navegador/*browser*; (2) HTML, CSS, Javascript e outras linguagens usadas para criar um *website*; (3) servidor web, que é o local onde os arquivos das linguagens acima ficam hospedados. Na maioria das situações, é por meio da web que uma pessoa acessa a Internet, com exceção de serviços como *e-mail*, FTP e troca de mensagens instantâneas.[207]

A partir desse momento, diversos atores públicos e privados com interesses não acadêmicos e não militares começaram a investir na Internet. Em 1990, a ARPANET é formalmente desligada. Diversas ferramentas de busca como Archie[208] e Gopher[209] aparecem. Jeff Bezos, por exemplo, começa a desenvolver o plano de mercado para a Amazon.com.[210] Bill Gates escreve o texto "O maremoto da Internet".[211] Em 1998, o Google é criado.[212] Essa popularização e profusão de produtores de conteúdo e consumidores de informações deu início à revolução digital, modificando profundamente a sociedade.

Para entender melhor a evolução dos usos e as potencialidades da Internet ao longo do tempo, costuma-se dividir a web em três gerações. A primeira geração (web 1.0), surgida em meados da década de 1980, ficou caracterizada pela possibilidade de conexão entre pessoas, porém de forma estática e sem uma interatividade com os *sites*, sendo estes criados somente para leitura (*read-only web*). A ausência de comunicação e de interação entre consumidores e produtores era algo inerente à web 1.0, mas apesar dessa característica soar tão negativa atualmente, isso não diminuiu seu impacto, pois pela primeira vez estavam

[207] OLHAR DIGITAL. Qual a diferença entre Internet e web? *Olhar Digital*, mar. 2014. Disponível em: <http://olhardigital.uol.com.br/noticia/qual-a-diferenca-entre-Internet-e-web/40770>. Acesso em: 27 mar. 2017.

[208] Cf. o site do mecanismo de busca disponível em: <http://archie.icm.edu.pl/archie-adv_eng.html>. Acesso em 17 jul. 2017 e STIEBEN, Danny. The Archie search engine – the world's first search! *Make Use Of*, may. 2013. Disponível em: <http://www.makeuseof.com/tag/the-archie-search-engine-the-worlds-first-search/>. Acesso em 17 jul. 2017

[209] O QUE É Gopher? *Canal Tech*, [s.d.]. Disponível em: <https://canaltech.com.br/produtos/O-que-e-Gopher/>. Acesso em: 17 jul. 2017.

[210] Cf. STONE, Brad. *The Everything Store*: Jeff Bezos and the Age of Amazon. Boston: Little Brown and Company, 2013.

[211] No original, "*The Internet tidal wave*".

[212] Disponível em: <https://www.google.com.br/about/our-story/>. Acesso em 17 jul. 2017.

disponíveis as mais variadas informações, gratuitamente, em milhões de páginas.[213] Outra característica da web 1.0 diz respeito à restrição dos aplicativos, que não podiam ser alterados ou ter seu funcionamento visualizado, sendo um dos principais exemplos o Netscape Navigator.

Para ilustrar, os primeiros *sites* de *e-commerce* encaixam-se na definição de web 1.0, pois eram apenas *sites* que disponibilizavam os catálogos em formato virtual, para que mais pessoas pudessem saber sobre seus produtos e serviços, de forma mais cômoda para o consumidor.[214]

É válido lembrar que o termo *web 1.0* foi cunhado apenas após a popularização do termo *web 2.0* por membros da O'Reilly Media em uma conferência realizada em 2004.[215] Dessa forma, surgiu uma necessidade de categorização e diferenciação entre essas duas eras.

A transição entre web 1.0 e web 2.0 não se deu de forma clara. Há uma linha tênue onde *sites* utilizam ferramentas inerentes a essas duas fases. Sendo assim, em alguns casos não é possível rotular um *site* como sendo 1.0 ou 2.0. Além do mais, dependendo de sua finalidade, alguns *sites* em formatos mais simples podem ser tão eficazes quanto os mais complexos.

Enquanto a web 1.0 ficou conhecida como a "web do conhecimento", pelo aumento súbito de informação que proporcionou aos usuários, a web 2.0 pode ser considerada a "web da comunicação", por conta da grande interatividade viabilizada em suas plataformas.[216] A mudança entre essas duas eras se deu por meio de uma nova forma de utilização das ferramentas que estavam disponíveis na web desde o início.

As principais características da web 2.0 fazem referência a seu caráter colaborativo e de interação constante dos usuários. Todas essas relações foram possíveis devido ao crescimento de plataformas como redes sociais, *blogs*, *wikis*,

---

[213] BIG THINK. Web 3.0. *Youtube*, abr. 2012. Disponível em: <www.youtube.com/watch?v=EMkTic4ztU8>. Acesso em: 27 mar. 2017.

[214] GETTING, Brian. Basic definitions: web 1.0, web. 2.0, web 3.0. *Pratical E-commerce*, abr. 2007. Disponível em: <www.practicalecommerce.com/articles/464-Basic-Definitions-Web-1-0-Web-2-0-Web-3-0>. Acesso em: 27 mar. 2017.

[215] Informações sobre a conferência, chamada de Web 2.0 Conference, podem ser conferidas no *site*, Disponível em:<http://conferences.oreillynet.com/web2con/>. Acesso em: 27 mar. 2017.

[216] AGHAEI, Sareh; NEMATBAKHSH, Mohammad Ali; FARSANI, Hadi Khosravi. Evolution of the world wide web: from web 1.0 to web 4.0. *Internet Journal of Web & Semantic Technology*, v. 3, n. 1, jan. 2012. Disponível em: <http://airccse.org/journal/ijwest/papers/3112ijwest01.pdf>. Acesso em: 27 mar. 2017.

entre outros. Dessa forma, a produção de conteúdo na Internet passou a ser realizada de maneira mais fluida. A partir do momento em que os próprios usuários puderam também abastecer as plataformas com informações, a web passou a ser uma via de mão dupla,[217] ganhando a denominação de *read-write* web. Portanto, com o advento da web colaborativa (2.0), o usuário de Internet deixou de ser somente um consumidor de conteúdo passando a ser, ao mesmo tempo, também produtor, dando origem ao conceito de *prosumer*,[218] típico das relações de interação nas plataformas de web 2.0, principalmente redes sociais.

Nessa fase de transição, também havia preocupações relativas à estrutura da web, a maioria delas concernentes ao tráfego de informações e coleta de dados, ou seja, não muito diferente dos obstáculos que o *boom* da IoT também promete proporcionar, porém, dessa vez, em escalas maiores.

Com relação aos *sites* de *e-commerce*, que na web 1.0 se apresentavam como algo análogo a catálogos, com o advento da web 2.0 esses mesmos *sites*, especialmente a Amazon.com, passaram a criar ferramentas de classificação dos produtos e abriram espaço para comentários dos usuários, fazendo com que a experiência da compra pudesse ser compartilhada com futuros consumidores.

Graham Cormode e Balachander Krishnamurthy buscaram explicar as principais diferenças entre a web 1.0 e a web 2.0:[219]

> A Web 2.0 captura uma combinação de inovações na Web nos últimos anos. É difícil encontrar uma definição precisa e é difícil categorizar muitos sites com o rótulo binário "Web 1.0" ou "Web 2.0". Mas há uma clara separação entre um conjunto de sites Web 2.0 altamente populares, como Facebook e YouTube, e a "web antiga". Essas separações são visíveis quando projetadas em uma variedade de eixos, como o tecnológico (o desenvolvimento de scripts e tecnologias de apresentação usadas para renderizar o site e permitir a interação dos usuários); estrutural (finalidade e disposição do site) e sociológico (noções de amigos e grupos).220

[217] RYAN, Johnny. *A history of the Internet and the digital future*. London: Reaktion Books, 2010, p. 150.
[218] GIURGIU, Luminita; BÂRSAN, Ghita. The prosumer: core and consequence of the web 2.0 Era. *Revista de Informatica Sociala*, ano V, n. 9, p. 53-59, jun. 2008.
[219] CORMODE, Graham; KRISHNAMURTHY, Balachander. Key diferences between web 1.0 and web 2.0. *First Monday*, v. 12, n. 6, jun. 2008. Disponível em: <http://firstmonday.org/ojs/index.php/fm/article/view/2125/1972>. Acesso em: 27 mar. 2017.
[220] Tradução livre do autor. No original: "*Web 2.0 captures a combination of innovations on the Web in recent years. A precise definition is elusive and many sites are hard to categorize with the binary label "Web 1.0" or "Web 2.0." But there is a clear separation between a set of highly popular Web 2.0 sites such as Facebook and YouTube, and the "old Web". These separations are visible when projected onto a variety of axes, such as technological (scripting and presentation*

Em seu reconhecido artigo sobre a conceituação de web 2.0, Tim O'Reilly criou uma tabela que procura exemplificar as principais mudanças entre essas duas primeiras gerações:[221]

Web 1.0	Web 2.0
DoubleClick	*Google AdSense*
Ofoto	*Flickr*
Akamai	*BitTorrent*
mp3.com	*Napster*
Britannica Online	*Wikipedia*
personal websites	*blogging*
Evite	*upcoming.org and EVDB*
domain name	*search engine optimization*
page views	*cost per click*
screen scraping	web *services*
publishing	*participation*
content systems	*wikis*
directories (taxonomy)	*tagging ("folksonomy")*
stickiness	*syndication*

Outra possibilidade de comparação entre as duas fases é a que se segue:[222]

Web 1.0	Web 2.0
Leitura	Leitura/escrita
Companhias	Comunidades
Cliente-servidor	*Peer to peer*
HTML, portais	XML, RSS
Taxonomia	Tags
Posse	Compartilhamento
IPOs	Transações
Netscape	Google
Web*forms*	Web *applications*
Screenscaping	APIs

technologies used to render the site and allow user interaction); structural (purpose and layout of the site); and sociological (notions of friends and groups)".

[221] O'REILLY, Tim. Design patterns and business models for the next generation of software. *O'Reilly*, set. 2005a. Disponível em: <www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1>. Acesso em: 27 mar. 2017.

[222] AGHAEI, Sareh; NEMATBAKHSH, Mohammad Ali; FARSANI, Hadi Khosravi. "Evolution of the world wide web: from web 1.0 to web 4.0", 2012, op. cit. p. 3.

Web 1.0	Web 2.0
Dialup	Banda larga
Custos de *hardware*	Custos de banda
Palestras	Conversação
Publicidade	Boca a boca
Serviços vendidos pela Internet	Serviços de web
Portais de informação	Plataformas

O termo *web 3.0*,[223] por sua vez, foi criado pelo jornalista John Markoff, do *New York Times*,[224] baseado na evolução do termo web 2.0 difundido por Tim O'Reilly e Dale Dougherty em 2004.

Enquanto a web 2.0 permitia a interação entre pessoas, a web 3.0 usará a Internet para cruzar dados. Essas informações poderão ser lidas pelos dispositivos e estes conseguirão fornecer informações mais precisas. O conceito de web 3.0 ainda é fluido e alvo de críticas, porém já apresenta algumas características que o distinguem das ondas anteriores. A principal delas são os novos polos de conexão, em que objetos interagem com pessoas e também com outros objetos; por isso a relação com a ideia de Internet "das coisas".[225]

Há uma forte indefinição no conceito de "coisa", muitas vezes entendido como sinônimo de "utensílio", atrelado à ideia de "aparelho, apetrecho, ferramenta, instrumento, peça, dispositivo, máquina, mecanismo, objeto ou petrecho". Outras vezes é usado como sinônimo de "objeto" que tampouco possui uma definição clara ou específica, podendo ser entendido segundo alguns dicionários como "tudo o que é exterior ao espírito; assunto, matéria, causa,

[223] RAY, Kate. Web 3.0. *Vimeo*, maio 2010. Disponível em: <https://vimeo.com/11529540>. Acesso em: 27 mar. 2017.
[224] MARKOFF, John. Entrepreneurs see a web guided by common sense. *The New York Times*, nov. 2006. Disponível em: <www.nytimes.com/2006/11/12/business/12web.html>. Acesso em: 27 mar. 2017. O texto foi traduzido para o português por Fabiano Caruso e pode ser encontrado em: <www.mail-archive.com/bib_virtual@ibict.br/msg01199.html>. Acesso em: 27 mar. 2017.
[225] É importante ressaltar o fato de que, com pontos em comum, a Internet das coisas faz parte da web 3.0, mas não se confunde com ela. A web 3.0, como o nome indica, consiste na terceira geração do conceito de web e compreende diferentes formas de integrar e analisar dados a fim de obter novos conjuntos de informações. O conceito de web 3.0 compreende características que fogem ao escopo da IoT, a exemplo das novas camadas na arquitetura da web. Há, ainda, mudanças na perspectiva das possibilidades de uso da web, que não necessariamente envolvem o uso de dispositivos inteligentes.

motivo; fim, escopo".[226][227][228]. Ainda, segundo o dicionário de Stanford, o termo "coisa" possui também um alcance amplo: "'*Thing', in its most general sense, is interchangeable with 'entity' or 'being' and is applicable to any item whose existence is acknowledged by a system of ontology, whether that item be particular, universal, abstract, or concrete. In this sense, not only material bodies but also properties, relations, events, numbers, sets, and propositions are — if they are acknowledged as existing — to be accounted 'things'*".[229]

Encontramos também uma definição dentro do âmbito jurídico relacionado ao Direito de Propriedade, diferenciando os conceitos de "coisa" e "bem". Parte considerável da doutrina[230] entende que "coisa" constitui um gênero, enquanto "bem" constitui espécie. Essa diferenciação foi adotada pelo Código Civi de 2002[231]. Os "bens", no direito civil, possuem classificação bem definida, vide artigos 79 a 103 do Código Civil.[232]

Há doutrinadores, no entanto, que compreendem esses conceitos no sentido oposto. Autores como Orlando Gomes, Teixeira de Freitas, Pablo Stolze e Rodolpho Pamplona Filho sustentam que bem é gênero e coisa é espécie. Existem ainda aqueles que seguem o pensamento de Washington de Barros, que diverge das duas correntes anteriores e leciona que por vezes coisas seriam gênero, outras

---

226 Disponível em: <https://www.priberam.com/dlpo/Objeto>. Acesso em: 27 mar. 2017.

227 Disponível em: <https://www.priberam.com/dlpo/objecto>. Acesso em: 27 mar. 2017.

228 Tradução livre do autor: Qualquer coisa que seja visível ou tangível e seja relativamente estável na forma; uma coisa, pessoa ou assunto a que o pensamento ou a ação são direcionados; o fim para o qual o esforço ou a ação são direcionados; objetivo; propósito. Disponível em: <http://www.dictionary.com/browse/object>. Acesso em: 27 mar. 2017.

229 Tradução livre do autor: A coisa, em seu sentido mais geral, é intercambiável com" entidade "ou" ser e é aplicável a qualquer item cuja existência seja reconhecida por um sistema de ontologia, seja esse item particular, universal, abstrato ou concreto. Nesse sentido, não só os corpos materiais, mas também as propriedades, as relações, os eventos, os números, os conjuntos e as proposições são, se forem reconhecidos como existentes, serem contabilizados

230 Dentre os doutrinadores que possuem esse posicionamento, por exemplo, Maria Helena Diniz e Silvio Venoza. Segundo essa corrente, portanto, Coisas são todos os objetos existentes – exceto as pessoas – ao passo que Bens são somente aquelas coisas de valor econômico. Em outra concepção, segundo Caio Mário da Silva Pereira: "Bem é tudo que nos agrada" (...) "Os bens, especificamente considerados, distinguem-se das coisas, em razão da materialidade destas: as coisas são materiais e concretas". DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro* Vol. 1. São Paulo: Saraiva, 2005. VENOSA, Sílvio de Salvo. *Direito Civil.* Direitos Reais. São Paulo: Atlas, 2013. PEREIRA, Caio Mario da Silva. *Instituições de Direito Civil* - Vol. II - Teoria Geral Das Obrigações. 28ª Ed. Forense, 2016.

231 Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 27 mar. 2017.

232 "Os bens são definidos como coisas ou objetos que possuem utilidade e servem para atender uma necessidade humana, eles podem ser trocados ou vendidos numa relação jurídica por causa de seu valor econômico ou pelo interesse que desperta. São classificados dentro do Código Civil dentro do livro 'Dos Bens'." Vide: DINIZ, Maria Helena, Curso de Direito Civil Brasileiro.

vezes seriam espécies, e em algumas ocasiões existe na verdade uma sinonímia. Em suas palavras: "Às vezes, coisas são gênero e bens, a espécie; outras estes são o gênero e aquelas, a espécie; outras, finalmente, são os dois termos usados como sinônimos, havendo então entre eles coincidência de significação."[233]

Sobre o conceito de coisa no enquadramento da IoT, vale mencionar a reflexão do especialista e pesquisador na área de tecnologia Silvio Meira:[234]

> Coisas, aqui, são dispositivos que têm, em alguma intensidade, capacidades de computação, comunicação e controle [...]. Se não tem sensores ou atuadores que lhe permitem características de controle, um objeto está no plano de computação e comunicação, é uma máquina em rede; se não tem capacidade de comunicação, é um sistema de controle digital; se não tem capacidades computacionais, é o que antigamente se chamava [e ainda existem, hoje] sistemas de telemetria. Coisas, aqui para nós, têm as três características, e todas elas digitais. A gente até poderia dizer que coisas, no sentido de Internet das *coisas*, são *objetos digitais completos*.

E continua:

> Mas é preciso dizer que as coisas, no verdadeiro sentido da *Internet das coisas*, são na verdade outras coisas – objetos físicos, sem qualquer das características acima, que são *envelopados por uma camada digital* que tem as características da imagem. E isso vai de uma lâmpada e uma fechadura até uma turbina e um veículo inteiro. Daqui pra frente, neste texto, coisas são a combinação de objetos físicos quaisquer com sua camada digital, normalmente inseparáveis. Lá na frente, pode ser que tal inseparabilidade seja uma propriedade dos *objetos digitais nativos.*[...] *As coisas não existem soltas, por aí.* E não são, ou não deveriam ser, simplesmente, sensores e atuadores em rede. isso seria diminuir muito o que se espera de *#IoT*, *the Internet of things*, e reduzir seu potencial ao da velha e boa telemetria. Para que todo [o] seu potencial possa ser capturado, *as coisas têm que fazer parte de um sistema*, de uma ou de um conjunto articulado de *plataformas*.

Considerando a amplitude conceitual dos termos "coisa" e "objeto" e considerando, ainda, a necessidade de despertarmos uma consciência crítica principalmente ao público não especializado no tema, entende-se que, apesar de ser de fato menos técnica a expressão 'Internet das *Coisas'* (alguns teóricos optam por 'Internet dos Dispositivos ou Internet dos Sensores'), essa nomenclatura atende melhor aos fins de capacitação para o debate em comparação à opção de pautarmos a abordagem nos conceitos técnicos de sensores ou objetos rastreáveis. Portanto, faremos a análise do fenômeno da IoT de forma ampla incluindo não

[233] Disponível em: <https://www.boletimjuridico.com.br/doutrina/texto.asp?id=2478>. Acesso em: 27 mar. 2017.
[234] MEIRA, Silvio. "Sinais do futuro imediato, #1: Internet das coisas", 2016, op. cit., grifos no original.

somente objetos físicos conectados, mas nos permitindo discutir também outros fatores e entidades que integram esse ecossistema, como a inteligência artificial, algoritmos, entre outros.

Talvez possamos afirmar que a principal diferença entre a web 2.0 e a web 3.0 está no fato de que a primeira foca na criatividade dos usuários para produção de conteúdo, uma vez considerados, ao mesmo tempo, consumidores e produtores das informações que trafegam *online*, enquanto a web 3.0 foca nos conjuntos de dados e objetos interligados.[235]

A tabela abaixo nos ajuda a visualizar algumas distinções importantes:[236]

Web 2.0	Web 3.0
Internet de leitura/escrita	Internet pessoal portátil
Comunidades	Indivíduos
Compartilhamento de conteúdo	Consolidação de conteúdo dinâmico
Blogs	Lifestream
AJAX	RDF
Wikipedia, Google	Dbpedia, igoogle
Tagging	Engajamento de usuários

Há quem defenda que a conexão entre máquinas (M2M) será cada vez mais útil para a organização de informações quando necessitarmos de respostas e soluções concretas e personalizadas. Essa tecnologia, potencializada com a conectividade cada vez maior dos dispositivos, proporcionará uma experiência diferenciada, com conteúdos mais inteligentes e focada no indivíduo. Especialistas acreditam que as utilidades da web 3.0 poderão nos proporcionar uma espécie de assistente pessoal,[237] que aprenderá cada vez mais sobre nós à medida que navegamos.

[235] AGHAEI, Sareh; NEMATBAKHSH, Mohammad Ali; FARSANI, Hadi Khosravi. Evolution of the world wide web: from web 1.0 to web 4.0, 2012, op. cit., p. 6.
[236] Ibid.
[237] "Por sua vez, o Santo Graal para os desenvolvedores da Web semântica é construir um sistema que possa dar uma resposta completa e razoável a uma pergunta simples como: 'Estou à procura de um local quente para passar as férias e disponho de US$ 3 mil. Ah, e tenho um filho de 11 anos'. No sistema atual, tal pergunta poderia levar a horas de pesquisa – por listas de voos, hotéis, aluguéis de carro – e as opções costumam entrar em conflito umas com as outras. Na Web 3.0, a

Junto com o conceito de web 3.0, surgiu também o conceito de *Internet semântica*. Tim Berners-Lee, o criador da *world wide web*, explica que a web semântica é um componente da web 3.0.[238] Durante as primeiras eras da Internet, todo o conteúdo era gerado para a compreensão de humanos, ou seja, as páginas da web são facilmente reconhecíveis para nós. Os computadores não possuíam essa habilidade, mas isso está mudando.

Com a Internet semântica, os dispositivos serão capazes de obter e interpretar as informações fornecidas pelos usuários. Agregando essas informações pessoais, as plataformas poderão individualizar os resultados. Exemplificando, mesmo que duas pessoas façam uma pesquisa utilizando os mesmos termos, os resultados serão diferentes, pois a busca utilizará também o histórico e o contexto de cada indivíduo.[239] A web 3.0 e a Internet semântica se sustentarão nas enormes bases de dados que serão criadas conforme os clientes utilizem as plataformas dotadas com as tecnologias dessa era.[240]

A web 3.0,[241] além de abarcar o conceito de web semântica, também possui outras características tão importantes quanto a que trata dessa web inteligente. Entre elas estão: a conectividade onipresente, também chamada de *ubiquitous computing*; as redes integradas e descentralizadas (computação em nuvem, P2P); tecnologias de código aberto (*open data, open source*); os cadastros

---

mesma pesquisa resultaria idealmente em um pacote de férias completo, planejado tão meticulosamente como se tivesse sido preparado por um agente de viagens humano" (MARKOFF, John. "Entrepreneurs see a web guided by common sense", 2006, op. cit.). O texto foi traduzido para o português por Fabiano Caruso e Disponível em: <www.mail-archive.com/bib_virtual@ibict.br/msg01199.html>. Acesso em: 27 mar. 2017.

[238] SHANNON, Victoria. A 'more revolutionary' web. *The New York Times*, maio 2006. Disponível em: <www.nytimes.com/2006/05/23/technology/23iht-web.html>. Acesso em: 28 mar. 2017.

[239] Como será visto ao longo deste estudo, a utilização de técnicas que se baseiam, entre outros dados, no histórico dos indivíduos, como *profiling* e *targeting*, pode gerar práticas que vão de encontro ao princípio da discriminação, o que deve ser evitado. Sobre o tema, confira-se: PEPPET, Scott R. Regulating the Internet of things: first steps toward managing discrimination, privacy, security, and consent. *Texas Law Review*, v. 93, p. 117-120, 2014; DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 173 e segs.

[240] SHADBOLT, Nigel; HALL, Wendy; BERNERS-LEE, Tim. The semantic web revisited. *IEEE Computer Society*, p. 96-101, maio/jun. 2006. Disponível em: <http://eprints.soton.ac.uk/262614/1/Semantic_Web_Revisted.pdf>. Acesso em: 28 mar. 2017.

[241] Ver vídeo ilustrativo sobre web 3.0. Disponível em: <www.youtube.com/watch?v=F_nbUizGeEY>. Acesso em: 28 mar. 2017.

integrados, nos quais é possível usar apenas uma conta para utilizar variados serviços.[242]

O quadro comparativo abaixo nos ajuda a distinguir as três fases:[243]

	Web 1.0	*Web* 2.0	*Web* 3.0
Comunicação	*Broadcast*	Interativa	Engajado/aplicado
Informação	Estática/apenas leitura	Dinâmica	Portátil & pessoal
Foco	Organização	Comunidade	Individual
Pessoal	*Home pages*	*Blogs*/*wikis*	*Lifestreams*
Conteúdo	Posse	Compartilhamento	Curadoria
Interação	*Web forums*	*Web applications*	*Smart applications*
Busca	Diretórios	Palavras-chave/*tags*	Contexto/relevância
Métrica	Visitas à pagina	Custo por click	Engajamento do usuário
Publicidade	Banners	Interativo	Comportamental
Pesquisa	*Britannica Online*	Wikipedia	*The semantic web*
Tecnologias	HTML/FTP	Flash/Java/XML	RDF/RDFS/OWL

Além da definição de IoT, relacionada aos conceitos mais recentes descritos anteriormente, também está sendo disseminado o conceito de *Internet de todas as coisas* ou *Internet de tudo* (*Internet of everything* – IoE).[244] Empresas como Cisco e Qualcomm, que trabalham com infraestrutura de redes, vêm difundindo esse termo em convenções e documentos. Porém, em princípio, não há diferenciações claras e substanciais entre os termos IoT e IoE. A própria

[242] LIFEBOAT FOUNDATION. Web 3.0: the third generation web is coming. *Lifeboat Foundation*: *Safeguarding Humanity*, [20--]. Special report. Disponível em: <http://lifeboat.com/ex/web.3.0>. Acesso em: 28 mar. 2017.

[243] WEB 3.0 & Beyond. *Rad Students Wiki*, [20--]. Disponível em: <http://rad-students.wikia.com/wiki/Web_3.0_%26_Beyond>. Acesso em: 28 mar. 2017.

[244] BAJARIN, Tim. The next big thing for tech: the Internet of everything. *Time*, jan. 2014. Disponível em: <http://time.com/539/the-next-big-thing-for-tech-the-Internet-of-everything/>. Acesso em: 28 mar. 2017.

Qualcomm não faz distinção nenhuma. Já a Cisco acredita que a IoT é um estágio de transição para que possamos alcançar a IoE.[245]

Definições e previsões sobre as próximas web*s* também já estão sendo realizadas. Alguns estudiosos apontam que a *web 4.0* ou *5.0* será uma web simbiótica,[246] capaz de integrar gradativamente as tecnologias ao ser humano, podendo envolver até sentimentos e emoções ou transformando a web em um cérebro paralelo ao nosso. As definições sobre as próximas web*s* são assumidamente vagas, visto que o termo *2.0* até hoje é alvo de críticas[247] e o conceito de web 3.0 ainda está se consolidando, mas as afirmações possíveis de serem feitas são sobre a maior utilização da inteligência artificial para criar uma web mais inteligente.

Tendo em vista a previsão de avanço deste contexto de hiperconectividade, exploraremos, a partir de agora, alguns aspectivos positivos e negativos da IoT no presente, tomando como referência a garantia dos princípios constitucionais. Esse balanço inicial nos permitirá aprofundar as problemáticas envolvendo o norteamento ético e a tutela dos dados nos capítulos seguintes.

1.2
Aspectos positivos da IoT: Benefícios Econômicos Estatais e Empresariais

A IoT tem sido encarada com otimismo por setores da indústria, podendo vir a se tornar um importante elemento econômico nas próximas décadas. A estimativa de impacto econômico global vinculado ao cenário de IoT corresponde a mais de US$ 11 trilhões em 2025.[248] Algumas estimativas antecipam cerca de 100 bilhões de dispositivos inteligentes conectados até aquele ano.[249]

---

[245] WEISSBERGER, Alan. Are the Internet of things (IoT) & Internet of everything (IoE) the same thing? *VIODI*, maio 2014. Disponível em: <http://viodi.com/2014/05/23/are-the-Internet-of-things-iot-Internet-of-everything-iot-the-same-thing/>. Acesso em: 28 mar. 2017.

[246] PATEL, Karan. Incremental journey for world wide web: introduced with web 1.0 to recent web 5.0: a survey paper. *International Journal of Advanced Research in Computer Science and Software Engineering*, v. 3, n. 10, p. 416, out. 2013.

[247] O'REILLY, Tim. Not 2.0? *Radar*, ago. 2005b. Disponível em: <http://radar.oreilly.com/2005/08/not-20.html>. Acesso em: 28 mar. 2017.

[248] ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. "The Internet of things: an overview. Understanding the issues and challenges of a more connected world", 2015, op. cit., p. 1; 4.

[249] Ibid., p. 4.

Em pesquisa realizada pela consultoria Accenture, estima-se que "a participação da economia digital no PIB do Brasil saltará dos atuais 21,3% para 24,3% em 2020 e valerá US$ 446 bilhões (R$ 1,83 trilhão)".[250] Segundo especialistas ouvidos pela BBC Brasil, conforme consta da mesma matéria[251]:

> O país se saiu bem na redução de desigualdade social na última década, mas precisa investir mais em educação e inovação para obter ganhos em produtividade e geração de empregos nesta nova economia: "O grande desafio à frente é manter os avanços sociais e estimular o aumento da produtividade", afirmou Alicia Bárcena, secretária-executiva da Cepal (Comissão Econômica para América Latina e Caribe), órgão ligado à ONU.

O Brasil se encontra na posição de número 57 do índice de competitividade mundial (World Competitiveness Yearbook) de 2016.[252] Esse é o principal relatório anual sobre a competitividade dos países publicado pelo pelo International Institute for Management Development (IMD) desde 1989. O anuário compara o desempenho de 63 países baseando-se em mais de 340 critérios que medem diferentes aspectos da competitividade.[253] Quanto ao índice global de inovação, o país está na posição de número 69.[254] Esse indicador mede o nível de inovação de cada país e é resultado de uma colaboração entre a Universidade Cornell, a INSEAD e a Organização Mundial de Propriedade Intelectual (WIPO). O índice global de inovação é parte de uma grande pesquisa que apresenta, por exemplo, os resultados das empresas, bem como a habilidade do governo de encorajar e suportar inovação por meio de políticas públicas.

Ou seja, tanto no aspecto de competitividade quanto no quesito de inovação, seja por via pública ou privada, o Brasil deixa a desejar. Fato é que a economia do país possui potencial para se desenvolver caso tenha as estruturas e

---

[250] WENTZEL, Marina. Quarta revolução industrial: como o Brasil pode se preparar para a economia do futuro. *BBC Brasil*, jan. 2016. Disponível em: <www.bbc.com/portuguese/noticias/2016/01/160122_quarta_revolucao_industrial_mw_ab>. Acesso em: 28 mar. 2017.

[251] Ibid.

[252] THE 2016 IMD World: competitiveness scoreboard. *IMD World Competitiveness Yearbook*, 2016. Disponível em: <www.imd.org/uupload/imd.website/wcc/scoreboard.pdf>. Acesso em: 28 jun. 2016.

[253] Mais informações sobre o índice de competitividade mundial podem ser conferidas no *site* oficial do International Institute for Management Development: <www.imd.org/wcc/world-competitiveness-center-rankings/world-competitiveness-yearbook-ranking/>. Acesso em: 8 maio 2017.

[254] DUTTA, Soumitra; LANVIN, Bruno; VINCENT-WUNSCH, Sacha (Ed.). *The global innovation index 2016*: winning with global innovation. Ithaca, Fontainebleau and Geneva: Cornell University, INSEAD and WIPO, 2016.

os incentivos necessários. É justamente nesse contexto que se deve pensar no cenário de hiperconectividade/Internet das coisas (IoT) visando aumentar a produtividade, levar à criação de novos mercados e incentivar a inovação.

A comunidade empresarial brasileira, inclusive, já percebeu o potencial da IoT. "Em recente pesquisa da Accenture com mais de 1.400 executivos C-level de 32 países, os entrevistados brasileiros revelaram estar muito conscientes das oportunidades que a IoT pode oferecer"[255] e destacaram, como os três principais benefícios esperados, o aumento na produtividade dos funcionários, o corte de custos e a otimização na utilização de seus bens. A melhor experiência dos consumidores também foi elencada como um dos benefícios esperados.[256]

Enxerga-se no desenvolvimento nacional do setor de serviços – área ligada à IoT – grande potencial, haja vista que o setor de serviços da economia brasileira representa mais de 70% do valor adicionado no país.[257] Este pode e deve ser desenvolvido a partir da IoT, com desdobramentos importantes para o restante da economia.

Em um estudo realizado em 2015,[258] os pesquisadores Mark Purdy, Ladan Davarzani e Armen Ovanessoff, de Harvard, fundamentam na teoria da difusão econômica a base teórica para que o Brasil possa sustentar todo o potencial que o desenvolvimento da IoT é capaz de trazer.

Segundo os pesquisadores, o desafio central do Brasil envolve o que eles chamam de "capacidade nacional de absorção" (CNA):[259]

> Com base em nossa pesquisa sobre épocas anteriores de ruptura tecnológica em entrevistas com especialistas em tecnologia, economia e negócios, identificamos quatro pilares que fundamentam a CNA de um país:

---

[255] PURDY, Mark; DAVARZANI, Ladan; OVANESSOFF, Armen. Como a Internet das coisas pode levar à próxima onda de crescimento no Brasil. *Harvard Business Review Brasil*, nov. 2015. Disponível em: <http://hbrbr.uol.com.br/como-a-Internet-das-coisas-pode-levar-a-proxima-onda-de-crescimento-no-brasil/>. Acesso em: 28 jun. 2016.

[256] ACCENTURE. *From productivity to outcomes*: using the Internet of things to drive future business strategies. 2015, p. 8. Disponível em: <www.accenture.com/t20150527T211103__w__/fr-fr/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/fr-fr/PDF_5/Accenture-CEO-Briefing-2015-Productivity-Outcomes-Internet-Things.pdf>. Acesso em: 28 jun. 2016.

[257] MOREIRA, Rafael. Em que atividades se concentram as empresas de serviços? *Economia de Serviços*, jun. 2016. Disponível em: <http://economiadeservicos.com/tag/estrutura-do-setor-de-servicos/>. Acesso em: 2 maio 2017.

[258] PURDY, Mark; DAVARZANI, Ladan; OVANESSOFF, Armen. "Como a Internet das coisas pode levar à próxima onda de crescimento no Brasil", 2015, op. cit.

[259] Ibid.

> 1. Os business commons representam o ambiente de negócios e o conjunto de recursos disponíveis para as empresas realizarem suas operações.
> 2. Os fatores de decolagem ajudam a criar massa crítica para a tecnologia se propagar além dos mercados de nicho, chegando a um grupo mais amplo de operadores em diferentes setores.
> 3. Os fatores de transferência permitem que uma tecnologia crie raízes muito mais profundas em uma economia – incluindo mudanças mais amplas no comportamento de empresas, consumidores e sociedade.
> 4. O dínamo da inovação entra em ação quando uma tecnologia produz inovação e desenvolvimento autossustentáveis.

Com isso, os autores afirmam que, atualmente, a CNA do Brasil é bastante insatisfatória. Citam, especificamente, a deficiência do capital humano, baixa infraestrutura (especialmente de comunicações), debilidade dos laços da economia brasileira com a economia global e problemas estruturais em políticas de pesquisa e desenvolvimento.

Levanta-se também a hipótese de que não basta para o Brasil apenas investir nos setores de serviços por meio da IoT. Deve haver conjuntamente a essa ação uma série de outras preocupações que envolvam, para além da infraestrutura da inovação nacional e educação, também as questões jurídicas e técnicas referentes a: (1) interoperabilidade entre as máquinas; (2) ética na comunicação máquina a máquina (M2M); (3) ética na utilização de dados pessoais dos usuários; (4) reavaliação do cenário de desenvolvimento tecnológico nacional (com implicação direta no sistema nacional de registro de patentes e transferência de tecnologia); (5) diagnóstico das políticas públicas na seara tecnológica do país.

A Internet Society,[260] em declaração recente, considerou a IoT como um fenômeno emergente de grande significado técnico, social e econômico.

> Produtos de consumo, bens duráveis, [...] componentes industriais e de utilidade pública, sensores e outros objetos do cotidiano estão sendo combinados com a conectividade da Internet e com capacidades analíticas de dados poderosas que prometem transformar a forma [como nós vivemos, tanto na esfera social quanto na profissional]. [261]

O impacto desse fenômeno vem sendo atrelado ao conceito, ainda em construção, de *quarta revolução industrial*. "As três revoluções industriais

[260] ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. "The Internet of things: an overview. Understanding the issues and challenges of a more connected world", 2015, op. cit., p. 1.
[261] Tradução livre do autor. No original: "*Consumer products, durable goods, (...) industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities that promise to transform the way we work, live, and play*".

anteriores tiveram início nos países desenvolvidos, chegando com atraso ao Brasil".[262] No fim do século XVIII, a primeira revolução foi iniciada, e água e vapor foram utilizados para mover máquinas na Inglaterra. A segunda, que teve início na metade do século XIX, veio do emprego de energia elétrica na produção em massa de bens de consumo. A terceira foi iniciada em meados do século passado e diz respeito ao uso da informática. A chamada "quarta revolução industrial", por sua vez, teria se iniciado na virada deste século e tem se construído a partir da revolução digital. Ela se caracteriza essencialmente por uma Internet ubíqua e móvel, por sensores e dispositivos que cada vez se tornam mais baratos e menores e pelo desenvolvimento da inteligência artificial.[263]

Exemplos da quarta revolução – associada por vezes ao contexto de "indústria 4.0" –[264] são as fábricas totalmente automatizadas que funcionam sem a interferência direta do homem. Todavia, a quarta revolução se configura para além disto – das máquinas inteligentes e conectadas – implicando também a fusão dos mais diversos tipos de tecnologias, em seus domínios tanto físicos quanto digitais.[265] Nessa revolução, a inovação prolifera de forma muito mais rápida entre os atores com condições de fomentá-la.

Em vista disso, pesquisadores[266] alertam para dois fatores capazes de limitar os potencias da nova revolução: (1) é necessário repensar os sistemas

[262] WENTZEL, Marina. "Quarta revolução industrial: como o Brasil pode se preparar para a economia do futuro", 2016, op. cit.
[263] Ibid.
[264] Apesar de comumente associados, os conceitos de indústria 4.0 e quarta revolução industrial são distintos. Revolução Industrial designa conjunto de drásticas alterações nos métodos de produção, com constituição de nova infraestrutura e aumento de produtividade num curto espaço de tempo. Até hoje, identificam-se três grandes marcos dessas mudanças na indústria, inicialmente a partir de sistemas físicos (primeira e segunda revoluções), chegando aos sistemas cibernéticos (terceira revolução). O momento seguinte, a saber, a quarta revolução industrial, prevê a criação de sistemas físico-cibernéticos (*ciber-physical systems*), utilizando, para isso, a Internet das coisas. Essa interação contínua entre dispositivos conectados e entre eles e os indivíduos promete ter grande impacto sobre a quantidade e os tipos de dados disponíveis, permitindo a criação de diferentes modelos de negócio *data-driven*. A indústria 4.0, por sua vez, tem origem na estratégia industrial do governo alemão a ser desenvolvida até 2020, que alia tecnologia aos meios de produção. Trata-se de manifestação da terceira revolução industrial, com evidentes implicações para a quarta. O modelo funda-se em seis princípios: capacidade de operação em tempo real, virtualização, descentralização, orientação à prestação de serviços, interoperabilidade e modularidade. Dessa forma, a quarta revolução marca novo momento na história da produção industrial no mundo, ao passo que a indústria 4.0 sinaliza a fase de transição entre os paradigmas industriais. Por tais razões, os dois conceitos ora expostos, apesar de intimamente ligados, têm distinções.
[265] SCHWAB, Klaus. *The fourth industrial revolution*. Genebra: World Economic Forum, 2016. p. 14.
[266] Ibid., p. 15.

econômicos, sociais e políticos para responder aos desafios que a indústria 4.0 impõe, visto que não há ainda uma diretriz institucional – tanto no nível nacional quanto no global – que norteie a forma de governar a difusão da inovação; (2) inexiste uma narrativa consistente, positiva e comum que destaque as oportunidades e desafios da quarta revolução, narrativa esta essencial para empoderar indivíduos e comunidades, com o intuito de evitar reações prejudiciais às mudanças que estão a caminho e potencializar os efeitos positivos de inovação e desenvolvimento.

A literatura recente tem apontado para o fato de que inovações tecnológicas e organizacionais estão surgindo juntas, de tal forma que levantam a esperança de uma "renascença" da atividade industrial nos países da OECD.[267] Em particular, mídias sociais e máquinas capazes de produzir pequenas quantidades de produtos de *design* a baixos custos têm trazido para o mercado uma camada de novas empresas inovadoras que têm o potencial de preencher os gargalos que foram abertos durante a grande recessão.

Sendo assim, estudos têm surgido para apontar as relações entre a competitividade do setor industrial e a qualidade de serviços-chave de suporte. Nordås e Kim,[268] por exemplo, observaram que, em países de baixa renda, o impacto da qualidade dos serviços e das políticas na competitividade é maior nas indústrias de baixa tecnologia; nos países de renda média, é maior nos setores de média tecnologia; em países de alta renda, o impacto é maior em indústrias de média e alta tecnologia.

Jorge Arbache[269] defende:

> A agenda dos serviços está ganhando relevância em razão da sua crescente importância para explicar o desempenho das empresas, o tipo de participação dos países nas cadeias globais de valor e o crescimento sustentado. O principal canal de transmissão entre a indústria e os serviços são as mudanças que ocorrem na natureza dos bens manufaturados, que estão se combinando com os serviços através de uma relação cada vez mais sinérgica e simbiótica para formar um

[267] NORDÅS, Hildegunn Kyvik; KIM, Yunhee. The role of services for competitiveness in manufacturing. *OECD Trade Policy Papers*, n. 148, p. 4, 2013. Disponível em: <http://dx.doi.org/10.1787/5k484xb7cx6b-en>. Acesso em: 29 mar. 2017.
[268] Ibid., p. 5.
[269] CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. *Serviços e competitividade industrial no Brasil*. Brasília: CNI, 2014. p. 9. Disponível em: <http://arquivos.portaldaindustria.com.br/app/conteudo_24/2014/12/09/517/ServioseCompetitividadeIndustrialnoBrasil.pdf>. Acesso em: 28 mar. 2017.

> terceiro produto, que nem é um bem industrial tradicional, nem tampouco um serviço convencional.

À medida que as coisas se tornam conectadas, podendo oferecer dados sobre seu uso efetivo pelos clientes-alvo, novos modelos de negócios, novos serviços e novos produtos tenderão a aparecer e neles haverá uma forte ligação entre serviço e produto, mudando substancialmente a relação entre produtor e consumidor. Nessa linha de raciocínio, "integrar os serviços ao núcleo das políticas industriais, tecnológicas, comerciais e de investimentos parece ser uma providência fundamental para elevar a competitividade industrial".[270]

O poder público demonstra já estar atento aos benefícios da IoT, entendendo que esta surge como importante ferramenta voltada para os desafios da gestão pública prometendo, a partir do uso de tecnologias integradas e do processamento massivo de dados, soluções mais eficazes para problemas como poluição, congestionamentos, criminalidade, eficiência produtiva, entre outros. Já existem exemplos de aplicações de IoT pelo país, e essas experiências tendem a aumentar.

Pela perspectiva federal, o poder público brasileiro, por meio de iniciativas do Ministério das Cidades e do Ministério de Ciências, Tecnologias, Inovações e Comunicações (MCTIC), já planeja a criação de planos nacionais que envolvem a IoT.

O primeiro deles foi proposto pelo Ministério das Cidades e prevê a criação de um projeto piloto de IoT no país, chamado Sistema Nacional de Identificação Automática de Veículos (Siniav).[271] Esse programa consiste na instalação de *tags* em veículos nacionais e importados com o intuito de permitir sua identificação por radiofrequência, facilitando a prevenção, fiscalização e repressão quanto ao roubo e furto de veículos e de cargas.[272-273]

---

[270] Ibid., p. 12.
[271] GOVERNO ADIA, mais uma vez, megapiloto de Internet das coisas no país. *TI RIO*, jun. 2015. Disponível em: <www.tirio.org.br/info/35868/governo-adia-mais-uma-vez-megapiloto-de-Internet-das-coisas-no-pais>. Acesso em: 25 jan. 2017.
[272] LEITÃO, Thais. Sistema de identificação automática de veículos entrará em funcionamento em janeiro. *EBC*, out. 2012. Disponível em: <www.ebc.com.br/2012/10/sistema-de-identificacao-automatica-de-veiculos-entrara-em-funcionamento-em-janeiro>. Acesso em: 4 maio 2017.
[273] Os *chips* deverão ser instalados numa frota estimada em 50 milhões de automóveis ativos, e o processo de identificação por radiofrequência ocorrerá por meio de dispositivo de identificação eletrônico instalado no veículo, antenas leitoras, centrais de processamento e sistemas informatizados de monitoramento.

Outro plano proposto pelo MCTIC, em parceria com o BNDES, tem um objetivo mais ambicioso. Procurar-se-ão definir as medidas a serem tomadas pelo país para que essa tecnologia seja promovida como um modelo de desenvolvimento de setores como o automobilístico, o agropecuário e o urbanístico. A partir de 2017, o governo brasileiro deu início a uma série de atividades voltadas para esse tema, incluindo grupos de trabalho e consultas públicas,[274] visando propor políticas e uma regulação para a IoT. A importância desse tipo de atividade está no desenvolvimento de um conjunto de leis que seja capaz de atender à inovação, característica da IoT, ao mesmo tempo que logra proteger direitos fundamentais.

Cabe ressaltar, ainda, que existe uma série de projetos federais no âmbito da infraestrutura de Internet. Esses programas objetivam ampliar a malha de fibra óptica brasileira, aumentando a qualidade do serviço de Internet que é oferecido. Ainda que tais projetos não sejam diretamente relacionados ao desenvolvimento e aplicação da IoT, sem a infraestrutura adequada os objetos inseridos no contexto da IoT não exercerão impacto significativo para a eficiência dos serviços nos setores público e privado.

Em relação aos planos de infraestrutura, é necessário destacar o programa Brasil Inteligente,[275] que tem por objetivo levar conexão de banda larga a 95% da população, universalizando o acesso à Internet no país. Esse programa é coordenado pelo MCTIC e possui três iniciativas básicas: o Minha Escola Mais Inteligente, o Programa Cidades Inteligentes e o Fundo Garantidor para Provedores Regionais.

O projeto Minha Escola Mais Inteligente é desenvolvido pela Eletrobras em parceria com o MCTIC. No entanto, ele permanece em fase de testes em Brasília e na Bahia. Seu objetivo é levar redes de fibra óptica a 30 mil escolas, elevando a velocidade dos acessos dos atuais 2 Mbps para 78 Mbps. A escolha

[274] É importante ressaltar que, atualmente, está aberta a primeira consulta pública sobre o Plano Nacional de Internet das Coisas. Espera-se que ainda neste ano de 2018 o governo federal apresente a versão final do projeto. Inclusive, o consórcio que inclui o CPqD e a consultoria McKinsey já apresentou uma consulta pública ao Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTI), uma proposta de estudo para oferecer os primeiros subsídios ao Plano Nacional de Internet das Coisas.

[275] O plano foi criado por meio do Decreto nº 8.776/2016 e representa uma nova fase do Programa Nacional de Banda Larga.

das escolas se dará com base no menor índice de avaliação e no menor custo de implantação da rede.

Outro programa interessante é a plataforma Estrutura Aberta de Tecnologias para Internet das Coisas e suas Aplicações,[276] que avalia, atualmente, 172 projetos de municípios interessados em implantar o uso da rede de fibras ópticas e soluções tecnológicas. O objetivo dessa plataforma é modernizar as gestões municipais.

Sob a ótica das perspectivas governamentais, é necessário ressaltar as iniciativas de São Paulo, Pernambuco, Paraná, Espirito Santo e Rio Grande do Sul,[277] que implementaram tecnologias dentro do âmbito da IoT como forma de aprimorar os serviços públicos oferecidos.

Destacam-se as iniciativas de utilização da IoT na área de segurança pública realizadas em alguns desses locais. Em Recife, por exemplo, está se desenvolvendo um dispositivo que tem capacidade de captar sons, ajudando na comunicação de arrombamentos, disparo de armas e até quedas de pacientes em hospitais.[278] Em Vitória (ES), o "botão do pânico" foi desenvolvido como forma de proteger as vítimas de violência doméstica, sendo esse um dos aplicativos utilizados dentro do escopo da IoT.[279] Em São Bernardo do Campo (SP) inaugurou-se o Centro Integrado de Monitoramento (CIM), um sistema com 400

[276] A plataforma "Estrutura Aberta de Tecnologias para Internet das Coisas e suas Aplicações" foi lançada em 2016 como parte do programa Cidades Inteligentes.

[277] O governo do Paraná decidiu investir em três áreas: água, luz e gás, criando redes inteligentes de energia elétrica, que vão reduzir o número e o tempo dos desligamentos na rede elétrica, medir o consumo de energia, água e gás a distância e descentralizar a geração de energia. Em teste na Grande São Paulo, está sendo implementado o sistema chamado Detecção e Vazamento de Água Potável (DVAP). O DVAP trabalha com três indicadores – pressão, vazão e ruído – para identificar mais precisamente onde está o problema. No setor de mobilidade urbana, em Curitiba, estão sendo colocados painéis eletrônicos nos pontos de ônibus, com horários de chegada. E em Porto Alegre (RS), sensores distribuídos pela cidade captam informações para monitorar os ônibus por GPS.

[278] PORTAL BRASIL. Microfone detecta arrombamentos e disparos de armas. *Portal Brasil*, abr. 2014. Disponível em: <www.brasil.gov.br/ciencia-e-tecnologia/2014/04/microfone-detecta-arrombamentos-e-disparos-de-armas>. Acesso em: 25 jan. 2017.

[279] ALMEIDA, Kamila. Projeto pioneiro no Brasil, botão de pânico ajuda a reduzir violência no ES. *ZH Notícias*, abr. 2013. Disponível em: <http://zh.clicrbs.com.br/rs/noticias/noticia/2013/04/projeto-pioneiro-no-brasil-botao-de-panico-ajuda-a-reduzir-violencia-no-es-4119173.html>. Acesso em: 25 jan. 2017; SMITH IV, Jack. Press this button and something will happen on the Internet. *Observer*, jan. 2015. Disponível em: <http://observer.com/2015/01/press-this-button-and-something-will-happen-on-the-Internet/>. Acesso em: 25 jan. 2017.

câmeras instaladas em áreas estratégicas, que transmitem imagens em tempo real durante as 24 horas do dia.[280; 281]

Em dezembro de 2016, o BNDES e o MCTI assinaram um acordo de cooperação técnica para elaborar o Plano Nacional de Internet das Coisas no Brasil, o qual irá definir as medidas a serem tomadas para que o país promova a chamada "Internet das Coisas" como modelo de desenvolvimento de setores como o automobilístico, agropecuário e urbanístico do país. Por meio de chamada pública, o consórcio que inclui o CPqD e a consultoria McKinsey apresentou ao Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTI) uma proposta de estudo para oferecer os primeiros subsídios ao Plano Nacional de Internet das Coisas. No ano de 2017, o governo brasileiro deu início a uma série de atividades voltadas ao tema, incluindo grupos de trabalho e consultas públicas visando uma regulação de Internet das Coisas que atenda à inovação ao mesmo tempo em que logra proteger direitos fundamentais.

Um dos principais desafios técnicos e regulatórios que o Brasil enfrentará a partir de agora relaciona-se ao papel do Estado na emergente realidade da hiperconectividade. O ecossistema regulatório brasileiro precisa ajustar-se rapidamente a esse cenário em transformação. O Estado deve aprovar regulações que protejam os direitos individuais, criem mercados eficientes e favoreçam a inovação de caráter nacional.

No setor privado, por sua vez, o entusiasmo com o potencial econômico da IoT vem dando margem a um forte investimento nessa área, tal como é percebido no setor *industrial IoT* ou *Internet das coisas industriais*, o qual é voltado para soluções de escala macro, como cidades inteligentes, rastreamento de carga, agricultura de precisão e gerenciamento de energia e ativos. Um exemplo desse tipo de investimento é o realizado pela empresa IBM, que não só investiu US$ 3

[280] DORADOR, Marcelo. Inauguração do Centro Integrado de Monitoramento em SBC. *ABC do ACB*, 2 abr. 2014. Disponível em: <www.abcdoabc.com.br/sao-bernardo/noticia/inauguracao-centro-integrado-monitoramento-sbc-18735>. Acesso em: 11 abr. 2017.

[281] Sobre o tema de *smart cities*, confira-se: PRADO, Eduardo. A Internet das coisas terá um papel fundamental nas cidades inteligentes. *Convergência Digital*, abr. 2015. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=38476&sid=15>. Acesso em: 25 jan. 2017; PORTAL BRASIL. "Microfone detecta arrombamentos e disparos de armas", 2014, op. cit.; ALMEIDA, Kamila. "Projeto pioneiro no Brasil, botão de pânico ajuda a reduzir violência no ES", 2013, op. cit.

bilhões em seu negócio de IoT[282] como também fez uma parceria com a AT&T[283] para fornecer soluções IoT industriais em uma série de questões, desde a eficiência energética até serviços de saúde.[284]

Essas novas frentes de investimento em IoT decorrem das perspectivas de lucro positivo do setor. Somente a título de exemplo, cabe ressaltar a pesquisa recente realizada pela Cisco que "estima que a Internet das Coisas pode adicionar 352 bilhões de dólares à economia brasileira até o final de 2022".[285] Por conta de previsões como essa, diversas empresas estão investindo mais em tecnologias IoT, desenvolvendo iniciativas concretas em diversas áreas.

Em relação às áreas em que essas tecnologias são empregadas, de 640 projetos de IoT anunciados, 22% deles são voltados para o ambiente da indústria conectada, um quinto para cidades inteligentes e 13% para o setor de energia e para carros conectados. A região que concentra a maior aplicação desse tipo de tecnologia é a americana, seguida pela Europa, e, por fim, pela Ásia e Oceania. É interessante notar, contudo, que em todos os campos de aplicação desses dispositivos se observa um crescimento no uso da tecnologia de IoT.[286]

No entanto, o investimento em IoT realizado por essas empresas pode não ser tão vantajoso se elas pretenderem expandir seus negócios. Nesse cenário, os custos em relação ao pagamento de *royalties* relacionados à propriedade intelectual e aos desafios de interoperabilidade passam a ser levados em conta, o que pode diminuir a margem de lucro.

Essas dificuldades explicam por que temos observado algumas empresas se aglomerarem em *clusters*, formando alianças e consórcios em torno de questões

[282] BASSI, Silvia. IBM transforma Internet das coisas em investimento estratégico bilionário. *Computer World*, ago. 2015. Disponível em: <http://computerworld.com.br/ibm-transforma-Internet-das-coisas-em-investimento-estrategico-bilionario>. Acesso em: 28 abr. 2017. Ver também relatório da Strategy Analytics disponível em: <www.strategyanalytics.com/>. Acesso em: 28 abr. 2017.

[283] SLOWEY, Lynne. AT&T and IBM partner for analytics with Watson. *IBM*, mar. 2017. Disponível em: <www.ibm.com/blogs/cloud-computing/2017/03/att-ibm-analytics-watson/>. Acesso em: 28 abr. 2017.

[284] Outras empresas, como a plataforma Watson IoT, combinam um ambiente de desenvolvimento e produção baseado em nuvem para aplicativos, *software* e serviços personalizados para indústrias específicas, além de análises cognitivas.

[285] DREHER, Felipe. IoT pode agregar US$ 352 bilhões à economia brasileira até 2022. *Computer World*, jun. 2015. Disponível em: <http://computerworld.com.br/iot-pode-agregar-us-352-bilhoes-economia-brasileira-ate-2022>. Acesso em: 25 jan. 2017.

[286] Os dados foram coletados a partir da tabela IoT Analytics. Disponível em: <https://iot-analytics.com/wp/wp-content/uploads/2016/08/List-of-640-IoT-projects-min.png>. Acesso em: 25 jan. 2017.

de IoT. Esses tipos de junções têm por objetivo potencializar os benefícios da IoT de forma a gerar uma estrutura única, segura, aberta e interoperável entre os produtos e serviços dessa tecnologia. Entre os *clusters* do setor, cabe destacar o Open Interconnect Consortium (OIC) e o AllSeen Alliance.

O OIC objetiva criar um novo padrão pelo qual bilhões de dispositivos, com e sem fio, se conectarão uns aos outros e à Internet por meio de uma arquitetura extensível. Em outras palavras, o OIC objetiva desenvolver padrões e certificações para dispositivos relacionados à IoT. Em 2014, ano de sua criação, o grupo era formado pelas empresas Intel, Broadcom e Samsung Electronics. Em 2016, a OIC mudou seu nome para a Open Connectivity Foundation e adicionou Microsoft, Qualcomm e Electrolux aos seus membros. Ser membro da OIC permite que as empresas se beneficiem de proteção de patentes de licenciamento cruzado.

Outra importante aliança de IoT, a AllSeen Alliance, que fornece a estrutura de IoT de código aberto AllJoyn, recentemente se fundiu[287] com a Open Connectivity Foundation, que patrocina o projeto *open source* da IoTivity.[288] Esse tipo de parceria tem o intuito de promover a interoperabilidade entre dispositivos conectados de ambos os grupos, permitindo um maior potencial operacional da IoT e expandindo o ecossistema de produtos conectados.

No âmbito internacional, algumas iniciativas relacionadas à IoT e sua utilização nos setores de transporte, agropecuária e pesquisa também merecem destaque.

No aeroporto de Düsseldorf, na Alemanha, por exemplo, para dar maior conforto aos passageiros e eficiência na prestação dos serviços, um robô manobrista realiza a função de encontrar e estacionar os veículos que chegam ao local. O robô realiza uma análise a *laser* que determina o tamanho e forma do carro para, em seguida, efetuar o reboque e armazenamento do veículo em uma

[287] ALLSEEN ALLIANCE MERGES with open connectivity foundation to accelerate the Internet of things. *Allseen Alliance*, Beaverton, out. 2016. Disponível em: <https://allseenalliance.org/allseen-alliance-merges-open-connectivity-foundation-accelerate-Internet-things>. Acesso em: 25 jan. 2017.

[288] Essa fusão terá a liderança das empresas AB Electrolux, Arçelik AS, ARRIS International plc, CableLabs, Canon, Inc., Cisco Systems, Inc., GE Digital, Haier, Intel, LG Electronics, Microsoft, Qualcomm, Samsung Electronics e Technicolor S.A.

vaga ideal. Além disso, o computador calcula e acompanha os detalhes do voo de volta do cliente para se programar e entregar o carro assim que o avião pousar.[289]

Cabe ressaltar, ainda no âmbito do transporte aéreo, que outros aeroportos utilizam a IoT em sistemas de reconhecimento facial para monitorar os movimentos dos passageiros dentro dos terminais, o que torna a passagem pelo controle de passaporte mais rápida.[290]

No setor agropecuário, as fazendas Tom Farms, nos Estados Unidos, desenvolvem atividade agrícola em escala industrial com ajuda da IoT.[291] Sensores nas colheitadeiras, serviços de GPS, tratores que se locomovem sozinhos e aplicativos que organizam a irrigação são exemplos de como a tecnologia é empregada.

Outros exemplos desse setor também podem ser observados na Itália,[292] local em que *startups* como a OMICAFARM utilizam aplicações de IoT para acompanhar o desenvolvimento da cultura. A tecnologia é capaz de localizar rapidamente áreas com água parada, definir processos de irrigação mais eficientes, identificar áreas com variação de biomassa, verificar informações como grau de radiação solar, temperatura do solo, pressão atmosférica e umidade relativa do ar.

No campo da pecuária, *startups* como a Smartbell também utilizam a tecnologia IoT para monitorar vacas e detectar sua fertilidade.[293] Esse tipo de

[289] MCCARTNEY, Scott. Viajante já pode testar aeroporto do futuro. *The Wall Street Journal*, jul. 2015. Disponível em: <http://br.wsj.com/articles/SB10836069722506714001504581112653322311690?tesla=y>. Acesso em: 25 jan. 2017.

[290] Ibid.

[291] Confira-se: ORO, David. Bytes and bushels: farming on an industrial scale. *IoT Central*, set. 2015. Disponível em: <www.iotcentral.io/blog/bytes-and-bushels-farming-on-an-industrial-scale?context=tag-farming>. Acesso em: 25 jan. 2017; HARDY, Quentin. Working the land and the data. *The New York Times*, Nova York, nov. 2014. Disponível em: <www.nytimes.com/2014/12/01/business/working-the-land-and-the-data.html#>. Acesso em: 25 jan. 2017; LOHR, Steve. The Internet of things and the future of farming. *Bits*, ago. 2015. Disponível em: <http://bits.blogs.nytimes.com/2015/08/03/the-Internet-of-things-and-the-future-of-farming/?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=3>. Acesso em: 25 jan. 2017.

[292] PRECISION FARMING to control irrigation and improve fertilization strategies on corn crops. *Libelium*, set. 1016. Disponível em: <www.libelium.com/precision-farming-to-control-irrigation-and-improve-fertilization-strategies-on-corn-crops/>. Acesso em: 25 jan. 2017.

[293] Confira-se: BYRNE, Michael. The Internet of cows is real. *Motherboard*, abr. 2016. Disponível em: <http://motherboard.vice.com/read/the-Internet-of-cows-Internet-of-things-agriculture>. Acesso em: 25 jan. 2017; MILES, Stuart. Internet of cows is now a thing as UK start-up creates cow tracking app. *Pocket-lint*, fev. 2016. Disponível em: <www.pocket-lint.com/news/136825-Internet-of-cows-is-now-a-thing-as-uk-start-up-creates-cow-tracking-app>. Acesso em: 25 jan. 2017.

monitoramento permite a identificação do momento mais adequado para a procriação.

No setor automotivo, um dos casos mais famosos de implementação da IoT é o dos carros da Tesla Motors.[294] Por meio deles, é possível conectar veículos a *smartphones* e verificar a bateria, localização por GPS, controlar o sistema de aclimatação, entre outras funcionalidades.

No campo da pesquisa, há de se destacar duas parcerias que objetivam ampliar e estudar o potencial da Internet das coisas. A primeira, realizada pela Huawei e pela PUC-RS,[295] se propõe a criar um novo sistema de iluminação pública, em que a tecnologia IoT empregada determinaria quando a luminária está queimada ou perto de queimar. A segunda foi a criação do projeto Inatel Smart Campus,[296] que tem por objetivo pesquisar e demonstrar projetos de Internet das coisas. A expectativa é que o projeto seja capaz de criar uma rede de conectividade em que as tecnologias relacionadas à IoT possam conversar entre si. Algumas aplicações já são desenvolvidas nesse projeto, tal como o sistema de iluminação inteligente.

O Campus está estruturado em mais duas frentes: (1) o *IoT lab*, que é voltado para alunos que desejam começar a testar projetos e aplicações com IoT e (2) a *smart house*, uma casa inteligente para demonstração dos projetos.

Esses exemplos denotam, em maior ou menor grau, o impacto da IoT no desenvolvimento de modelos de negócio bem-sucedidos no setor privado e algumas soluções inovadoras para problemas no setor público. É importante, no entanto, que ambos os setores tenham a clareza de que a tecnologia IoT ainda é um mercado recente a ser explorado e devidamente regulamentado, necessitando ser promovido por ações político-econômicas capazes de ampliar o crescimento econômico e o desenvolvimento nacional.

---

[294] Confira-se: BRISBOURNE, Alex. Tesla's over-the-air fix: best example yet of the Internet of things? *Wired,* [201-]. Disponível em: <www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-Internet-things/>. Acesso em: 25 jan. 2017; THE TESLA IOT car: case study. *MITCNC Blog*, ago. 2014. Disponível em: <https://blogmitcnc.org/2014/08/21/the-tesla-iot-car-case-study/>. Acesso em: 25 jan. 2017.

[295] IT FORUM (Redação). Huawei e PUCRS abrem centro de inovação com foco em cidades inteligentes e IoT. *IT Forum*, abr. 2016. Disponível em: <http://itforum365.com.br/noticias/detalhe/119237/huawei-e-pucrs-abrem-centro-de-inovacao-com-foco-em-cidades-inteligentes-e-iot>. Acesso em: 25 jan. 2017.

[296] UM CAMPUS ABERTO à pesquisa e testes para mercado de IoT. *Inatel*, set. 2016. Disponível em: <www.inatel.br/imprensa/noticias/pesquisa-e-inovacao/2938-um-campus-aberto-a-pesquisa-e-testes-para-mercado-de-iot>. Acesso em: 25 jan. 2017.

Exploraremos, no item seguinte, alguns aspectos negativos relacionados ao contexto de IoT, tecendo reflexões críticias iniciais ao fenômeno, o que nos permitirá aprofundar os aspectos regulatórios à frente.

1.3
Aspectos Negativos da IoT: Reflexões Críticas ao Fenômeno

A Internet foi projetada para resistir a uma explosão nuclear. Mas não a um ataque de torradeiras.[297]

A expansão e aperfeiçoamento da Internet das Coisas nos traz inúmeros benefícios, tais como as facilidades em ter todas as nossas informações conectadas umas às outras, nos dando pronto acesso aos serviços que necessitamos e nos trazendo mais comodidade. Segundo Philip N. Howard, professor de comunicação e escritor, através desse fenômeno, daremos início a uma era chamada por ele por "*Pax Techinica*"[298].

Segundo a sua teoria, os atuais sistemas de governo soberanos darão lugar a "sócio-tecnocracias" baseadas em intensivos informes sobre os dados relativos aos nossos comportamentos, hábitos e crenças, os quais serão transmitidos por meio de dispositivos, tais como *smartphones, tablets, smart TVs*. Segundo Philip, não precisaremos mais expressar nossas crenças e valores, visto que nossos dados comportamentais já farão isso por nós[299].

No entanto, essa interconectividade pode trazer uma enorme gama de problemas e questões discutíveis, dentre elas, as fragilidades em relação à privacidade e à segurança dos usuários. Como proceder em um contexto dependente da tecnologia se a mesma está vulnerável a interferências? Qual deve ser o papel do Estado e das empresas fornecedoras desses serviços?

Com o crescimento exponencial do universo digital, haverá um aumento na produção e tratamento de dados, e isso impactará profundamente a relação

[297] Frase adaptada da fala de Jeff Jarmoc. No original: "*In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters".* Disponível em: <https://twitter.com/jjarmoc/status/789637654711267328?lang=pt>. Acesso em: 03 abr. 2017.
[298] HOWARD, Philip. *Pax Techinica.* New Haven: Yale University Press, 2015.
[299] Ibid.

existente entre consumidores, máquinas e empresas. Alguns desafios quanto à segurança de dados no contexto da IoT já vêm sendo debatidos e alardeados por especialistas[300]. O ritmo no qual as tecnologias, especialmente no âmbito da IoT, estão avançando é acelerado e, até o momento, as empresas não conseguiram garantir suficientemente a segurança e a privacidade dos dados, com a mesma velocidade e empenho com que vem desenvolvendo os dispositivos de IoT.

Com relação à segurança dos dados não há ainda um consenso entre os fabricantes de produtos de IoT. Os próprios desenvolvedores ainda não possuem uma noção completa do que é realmente necessário em termos de segurança. A fórmula indicada é continuar com a prática de testes de vulnerabilidade em *softwares* e sistemas, além de também conscientizar os usuários a manterem sempre os seus dispositivos atualizados com as ferramentas de segurança acessíveis.

O desafio da segurança de dados no cenário de IoT envolve também dar enfoque em questões como gestão de armazenamento, servidores e redes de *data center*, bem como na responsabilidade de cada empresa que opere nessa cadeia de produtos e serviços. Isso ocorre por conta do crescimento dos dispositivos conectados, o que aumenta o volume de dados capturados e de operadores que atuam nesta cadeia econômica.

Tendo em vista que a IoT abrange diversos setores, alguns deles delicados como saúde e meio ambiente, isso nos faz crer que deverão surgir novos desafios de segurança envolvendo o grande fluxo de dados, sendo necessário acompanhar a complexidade da segurança no tratamento de *Big Data*.

Pesquisas recentes realizadas sobre o tema demonstram graves falhas de segurança com relação a aparelhos ligados à IoT. A HP Security Research[301] detectou em seu estudo que 70% dos dispositivos possuem falhas de segurança, estando propensos a ataques de *hackers*. Os principais problemas encontrados foram os de privacidade, autorizações insuficientes, falta de criptografia no transporte de dados, interface *web* insegura e softwares de proteção inadequados.

[300] DONEDA, Danilo, ALMEIDA, Virgílio; MONTEIRO, Marilia. Governance challenges for the Internet of Things. *IEE Computer Society*, v. 19, n. 4, p. 56-59, 2015.
[301] HEWLETT-PACKARD COMPANY. *Internet of Things Research Study Report*, jul. 2014. Disponível em: <http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VZRsHflVhHw>. Acesso em: 08 fev. 2017.

Na indústria automobilística, por exemplo, o crescente uso da tecnologia nos automóveis e sua integração com outros dispositivos nos trazem benefícios. O uso do GPS, controle por voz, sistema de câmeras, entre outros avanços são de grande utilidade em nosso dia a dia. Por outro lado, essa tendência de automatização os deixam mais suscetíveis a interferência de *hackers*.

As possibilidades de hackeamento de veículos são múltiplas. Pode ocorrer de forma geral ou direcionada (com acesso interno ou remoto), com milhares de automóveis ou apenas em um determinado, podendo também ser direcionado a sistemas específicos destes. De certa forma, essa é uma questão bem mais problemática que o hackeamento de smartphones, por exemplo. Nesse caso, não está em risco apenas as informações pessoais do motorista (rotas utilizadas, velocidade média, estações de rádio acessadas etc.), mas sim a sua vida e a do passageiro. Em outras palavras, em um carro hackeado, o motorista pode perder toda sua autonomia sobre o automóvel - seus comandos não serão mais aceitos.

Cabe ressaltar que, recentemente [302], hackers norte-americanos encontraram uma falha na tecnologia Uconnect, que consiste em um sistema conectado à Internet presente em milhares de carros da marca Fiat Chrysler. Os *hackers* conseguiram acessar o sistema operacional dos automóveis através de um chip central dos veículos, o que lhes dá acesso ao computador interno do carro, permitindo a interferência até nas suas partes mecânicas, como o freio e aceleradores.

Outras áreas também apresentam graves ameaças ao consumidor. Alguns casos exemplificativos podem ser citados como o das *Smart TVs*. O analista David Jacoby, da Kaspersky Lab, em seu estudo, "Internet das coisas: Como hackeei Minha Casa" [303], testou alguns aparelhos domésticos e detectou falhas que permitiam o acesso remoto às televisões. Isso se tornou mais preocupante desde a descoberta de que as *Smarts TVs* da Samsung capturavam as conversas pessoais

[302] De longe, hackers 'invadem' e controlam carro com jornalista dentro. Disponível em: < https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>. Acesso em 30 mar. 2017.
[303] JACOBY, David. Pesquisa: Como hackeei minha casa. *Kaspersky Lab*, 22 ago. 2014. Disponível em: <https://blog.kaspersky.com.br/pesquisa-como-hackear-minha-casa/3804/> Acesso em: 30 mar. 2017.

dos usuários utilizando sua funcionalidade de ativação por voz e coletavam o histórico de programas assistidos, tudo isso sem a permissão do consumidor[304].

Em uma escala maior de impacto, é necessário explicitar os ataques de *hackers* que ocorreram em outubro de 2016 e janeiro de 2017. O primeiro caso atingiu grandes sites como Netflix, Spotify e PayPal, os quais ficaram fora do ar em virtude de ataques DDoS. O alvo desta investida foi o Dyn[305], companhia que controla boa parte dos domínios da Internet[306]. Os *hackers* fizeram um ataque coordenado que consiste na sobrecarga da largura da banda de determinado *site* até que os recursos dele se esgotem, utilizando técnicas para enviar pedidos de pacotes em volume muito maior do que o normal. Nesse tipo de ataque, os servidores ficam instáveis ou até mesmo inacessíveis por não conseguirem responder a tantas requisições maliciosas[307]. O segundo caso ocorreu há poucos dias da posse do presidente Donald Trump na capital americana e fez uso de um código malicioso denominado *ransomware*. Esse código, que torna inacessíveis as informações de um determinado equipamento[308], impossibilitou o acesso aos dados das câmeras da polícia de Washington entre os dias 12 e 15 de janeiro[309].

O acontecimento teve grandes proporções pois muitos dispositivos IoT – como câmeras de segurança – foram utilizados para chegar ao servidor DNS Dyn[310]. Os atacantes se aproveitaram da baixa segurança destes dispositivos para infectá-los com o *malware botnet*. Quanto mais dispositivos afetados, maiores os

---

[304] *O Globo*. Samsung adverte: Cuidado com o que você diz em frente a sua TV inteligente. 09 fev. 2015. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/samsung-adverte-cuidado-com-que-voce-diz-em-frente-sua-tv-inteligente-15286181> Acesso em: 30 mar. 2017.

[305] DNS Dyn ou dinâmico (DDNS) é um método para atualizar automaticamente um servidor de nomes no Domain Name System (DNS).

[306] LOVELACE JR., Berkeley e VIELMA, Antonio José. Friday's third cyberattack on Dyn 'has been resolved', company says. *CNBC*, 21 out. 2016. Disponível em: <http://www.cnbc.com/2016/10/21/major-websites-across-east-coast-knocked-out-in-apparent-ddos-attack.html>. Acesso em: 08 fev. 2017.

[307] PAYÃO, Felipe. Quebrando a Internet: estamos sofrendo o maior ataque DDoS da história. *Tecmundo*, 21 out. 2016. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/110842-grande-ataque-ddos-afeta-twitter-psn-spotify-outros-estragos.htm>. Acesso em: 30 mar. 2017.

[308] CENTRO DE ESTUDOS, Resposta e Tratamento de Incidentes de Segurança no Brasil. *Cartilha de Segurança para Internet*, [201-?]. Disponível em: <http://cartilha.cert.br/ransomware/>. Acesso em: 30 mar. 2017.

[309] WILLIAMS, Clarence. Hackers hit D.C. police closed-circuit camera network, city officials disclose. *The Washington Post*, 27 jan. 2017. Disponível em: <https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.3dc5da77508f> Acesso em: 30 mar. 2017.

[310] DNS Dyn ou dinâmico (DDNS) é um método para atualizar automaticamente um servidor de nomes no Domain Name System (DNS).

danos ao servidor. Após o evento, inúmeros sites apontaram a vulnerabilidade da IoT como verdadeira ameaça à manutenção da Internet e reclamaram providências no sentido de proteger melhor os dispositivos[311].

Para o teórico Scott R. Peppet[312] os objetos de IoT são mais suscetíveis a falhas na segurança e a invasão por *hackers* por conta de três motivos. O primeiro seria um problema de caráter estritamente de conhecimento técnico, já que boa parte das empresas que pretendem atuar no cenário de IoT não são especializadas no desenvolvimento de *software* ou *hardwares* de alto nível, mas sim de produção de bens de consumo relativamente comuns no mercado. Para o autor, isso poderia significar que os engenheiros envolvidos com o projeto desses produtos fossem inexperientes em relação ao desenvolvimento de sistemas de segurança de alto nível.

O segundo seria que esses tipos de objetos, geralmente, tem uma forma compacta, o que dificulta que eles tenham a capacidade de processamento necessária para um sistema de segurança de dados eficiente. Além disso, alguns objetos inseridos no cenário de Internet das Coisas algumas vezes têm um tamanho tão reduzido que a sua bateria não é suficiente para processar sistemas de segurança de dados complexos.

O terceiro seria que grande parte dos objetos de IoT não são desenvolvidos com o intuito de serem atualizados frequentemente para aprimorar os seus sistemas de segurança de dados.

Além dos riscos relacionados a segurança, é possível ainda, no cenário de IoT, refletir sobre potenciais ameaças a proteção de dados pessoais. Os autores Jan Ziegeldorf, Oscar Morchon e Klaus Wehrle, em seu texto "*Privacy in the Internet of Things: Threats and Challenges*", identificam algumas ameaças relacionadas a diferentes fases de utilização da tecnologia, sendo essas as fases de coleta, processamento e disseminação das informações[313].

---

[311] THE GUARDIAN. DDoS attack that disrupted Internet was largest of its kind in history, experts say. *The Guardian*, out. 2016. Disponível em: <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>. Acesso em: 30 mar. 2017.

[312] PEPPET, Scott R. Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, v. 93, n. 85, p. 85-176, 2014.

[313] Na fase de coleta corre a obtenção de dados do usuário. Na fase de processamento ocorre a compilação das informações de localização do usuário. Por fim, na fase de disseminação de informações ocorre o compartilhamento de determinados dados.

O primeiro risco seria o da identificação. Isto é, da associação de um conjunto específico de dados a identidade de alguém. Essa ameaça estaria mais presente na fase de processamento das informações, mas pode ocorrer também durante outras fases do ciclo da tecnologia. Para os autores, as tecnologias inseridas no contexto de IoT seriam mais sujeitas a esse risco devido às possibilidades de identificação facial e por meio das digitais do indivíduo.

Sobre a identificação facial, uma interessante e controversa iniciativa para chamar atenção para a vulnerabilidade de dispositivos de IoT consiste na plataforma *Insecam*. Acessando o site "*http://www.insecam.org/*", o usuário tem imediatamente à sua frente, acesso a milhares de câmeras de diferentes países conectadas à Internet, invadidas apenas por possuírem senhas padrão. A ideia do *site*, no entanto, é criar um alerta para a privacidade online e a importância de mudar as senhas a partir da exposição não autorizada destas imagens[314]. Há filmagens de pessoas assistindo TVs em salas de estar, crianças dormindo em suas camas, bem como imagens de garagens, bairros, escritórios de empresas, entre outros.

O site possui imagens abertas, e em tempo real, de 11.000 câmeras nos EUA, cerca de 2.500 no Reino Unido, seis na Tanzânia e outras em todo o mundo. Não somente os locais dessas câmeras são indicados, como também os marcadores de latitude e longitude e um link para o *Google Maps* de onde se encontra a casa ou o estabelecimento.

Ademais, há de se ressaltar o fato de que as empresas, durante anos, passaram a confiança aos usuários de que seus dados estariam seguros através de ferramentas de anonimização. No entanto, cientistas vem demonstrando ao longo dos últimos 15 anos a facilidade de se re-identificar dados anonimizados[315].

O autor Scott R. Peppet em seu artigo "*Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent",*

[314] Empresas de câmeras de segurança bem conhecidas como a Foscam, a Linksys e a Panasonic pré-programam *logins* e senhas simples para seus usuários durante a configuração inicial dos produtos e deixam a opção dos próprios usuários redefinirem suas senhas posteriormente, mas sem informar o usuário da importância disto.

[315] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, v. 57, p. 6, 2010.

aponta que um dos principais problemas de privacidade nos produtos inseridos no cenário de IoT seria a ilusão da anonimização[316].

É bem verdade que essa problemática da falsa anonimidade dos dados não é um problema exclusivo desse tipo de tecnologia, estando presente na maior parte dos serviços e produtos de que os indivíduos fazem uso cotidianamente. O teórico Paul Ohm, em seu artigo "*Broken Promises of Privacy: responding to the surprising failure of anonymization",* ao tratar sobre os riscos para a privacidade, já criticava o fato de se acreditar piamente na anonimização dos dados[317].

Ainda que um dado tenha sido suprimido para garantir a privacidade do usuário, um adversário (como é chamado na literatura científica) pode reidentificá-lo (ou desanonimizá-lo) por meio do cruzamento de outras informações sobre o usuário disponíveis na Rede. Isso pode, inclusive, acarretar a descoberta da identidade real da pessoa[318]. Nas palavras de Ohm[319]:

> A reconfiguração fácil representa uma mudança radical não apenas na tecnologia, mas também na nossa compreensão da privacidade. Ela enfraquece décadas de suposições sobre a anonimização robusta, suposições que traçaram o curso para relações de negócios, escolhas individuais e regulações governamentais.[320]

No contexto de IoT, Peppet argumenta que, mesmo que o conjunto de dados coletados pelos sensores sejam considerados esparsos, a reidentificação ainda seria possível. Isso ocorre porque os sensores podem captar uma multiplicidade de informações de forma tão rica, correlacionando diferentes tipos de dados, que cada indivíduo possui uma espécie de "marca" que o diferencia dos outros usuários.

O segundo risco é o de rastreamento, permitindo-se identificar a localização de um indivíduo em determinado espaço e tempo. O acesso ao conteúdo seria mais comum na fase de processamento, tendo em vista que é nessa

---

[316] PEPPET, Scott R. Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, vol. 93, n. 85, p. 85-176, 2014.
[317] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, v. 57, p. 1701-1777, 2010.
[318] Ibid.
[319] Ibid.
[320] Tradução livre do autor. No original: "*Easy re-identification represents a sea change not only in technology but also in our understanding of privacy. It undermines decades of assumptions about robust anonymization, assumptions that have charted the course for business relationships, individual choices, and government regulations."*

fase que as informações de localização do usuário são compiladas sem que ele tenha o controle.

Ainda para Jan Ziegeldorf, Oscar Morchon e Klaus Wehrle, em texto anteriormente citado, o principal receio de diversos estudiosos de IoT, se deve ao fato de que os usuários não têm o controle sobre esse tipo de dado. Ele é, muitas vezes, disponibilizado sem o seu consentimento, ou a informação é utilizada e combinada com outras de forma inapropriada[321].

Outro ponto ressaltado pelos autores é o grau de percepção dos usuários em relação à existência desses sensores. Eles explicitam que os objetos inseridos na tecnologia de IoT sofreriam relativas diminuições, dificultando a percepção do usuário sobre eles para saber se a sua localização está sendo rastreada ou não.

O terceiro risco apontado pelo autor remete-se ao *profiling,* o que pode ser explicitado pela criação de dossiês de informações sobre determinado indivíduo com o intuito de efetuar correlações com outras informações e perfis. Esse risco à privacidade aparece na fase de disseminação, quando determinados dados são compartilhados com terceiros ou quando alguma decisão por parte da empresa é realizada de forma errônea.

Para os já mencionados autores, existe também um risco durante a liberação de informações para indivíduos não autorizados pelo usuário, tal como o denominado *"shoulder surfing*"[322]. Essa preocupação também é ressaltada por Antonio F. Skarmeta, José Ramos e Victoria Moreno, em seu artigo "*A decentralized approach for security and privacy challenges in the Internet of Things*". Uma tecnologia sugerida foi o *Fi-Ware*, que é um sistema ligado a mecanismos de autorização e autenticação de dados, o que inclui a criação de um conjunto de atributos e credenciais necessários para se ter acesso às informações. Segundo os pesquisadores[323]:

> Ele também inclui uma linguagem de política de tratamento de dados que define como os dados solicitados são manipulados e para quem eles são transmitidos, fornecendo os meios para liberar e verificar esses atributos e credenciais. (...) Também é importante considerar os mecanismos que permitem a proteção de

[321] ZIEGELDORF Jan, Morchon Oscar, Wehrle Klaus. Privacy in the Internet of Things: Threats and Challenges. *Revista Security and Communication Networks*, vol. 7, n. 12, p. 2728- 2742, 2013.
[322] Ibid.
[323] SKARMETA, Antonio, RAMOS José; MORENO, Victoria. *A decentralized approach for security and privacy challenges in the Internet of Things*. Apresentado no IEE World Forum, 2014.

> informações baseadas em algoritmos de criptografia dentro do armazenamento seguro.[324]

O quarto risco à privacidade dos usuários pode ocorrer durante as mudanças de controle do *lifecycle* da tecnologia se for liberada alguma informação pessoal do usuário. As transições de *lifecycle* ocorrem por conta das informações coletadas e armazenadas, por isso a ameaça reside no processo de coleta dessas informações. Os autores explicitam que o *lifecycle* da maior parte dos bens tecnológicos atualmente está inserido no modelo "*compre uma vez e seja dono para sempre"*, o que não será tão comum no cenário de Internet das Coisas. Os objetos inseridos na tecnologia IoT terão um *lifecycle* bem mais dinâmico, no qual os objetos serão descartados, modificados e emprestados de uma forma mais flexível.

Os estudiosos Radomirovic[325] e Van Deursen[326] já reconheceram o risco de criação de perfis pessoais por meio de impressão digital em tecnologia RFID (sistema de radiofrequência). Além disso, de acordo com Ziegdorf:[327]

> Com RFID o problema está em um âmbito muito mais local, visto que tags RFID podem ser lidas apenas a partir de uma distância curta e consultas são, em sua maior parte, restritas à leitura do identificador da tag. Como analisado acima, o problema será agravado com a evolução da IoT, pois o vetor de ataque é muito ampliado pelo aumento da proliferação de comunicações sem fio, conectividade de ponta a ponta e consultas mais sofisticadas.[328]

Os principais desafios técnicos para esse risco à privacidade demandam a criação de questionários de autenticação de identidade, bem como a criação de mecanismos robustos de identificação por meio de impressão digital.

---

[324]Tradução livre do autor. No original: "*It also includes a data handling policy language that defines how the requested data are handled, and to whom they are passed on, providing the means to release and verify such attributes and credentials. (...) It is also important to consider the mechanisms enabling the protection of information based on encryption algorithms within the secure storage*."

[325] RADOMIROVIC, S. *Towards a model for security and privacy in the internet of things*. I International Workshop on the Security of the Internet of Things, Tóquio, 2010. Disponível em: <www.caad.arch.ethz.ch/noolab/files/external/conferences/IoT2010_proceedings/pdf/WS1/WS1_9.%20seciot2010_submission_10_final_v0.pdf>. Acesso em: 8 set. 2017.

[326] VAN DEURSEN, T. 50 ways to break RFID privacy. Privacy and identity management for life. *IFIP Advances in Information and Communication Technology*, v. 352, p. 192-205, 2011.

[327] ZIEGELDORF, Jan; MORCHON, Oscar; WEHRLE, Klaus. "Privacy in the internet of things: threats and challenges", 2013, op. cit.

[328] Tradução livre do autor. No original: "*With RFID the problem is at a much more local scope as RFID tags can be read only from a close distance and queries are mostly restricted to Reading the tag's identifier. As analyzed above, the problem will aggravate in the IoT evolution as the attack vector is greatly increased by increasing proliferation of wireless communications, end-to-end connectivity, and more sophisticated queries*."

No cenário de *IoT*, o sistema de RFID é uma das formas de coleta de informação mais utilizadas. Os autores Carlo Maria Medaglia e Alexandru Serbanati, em seu artigo "*An Overview of Privacy and Security Issues in The Internet of Things"* explicitam que as formas de coleta de informação e identificação do usuário podem se dar de duas maneiras: por esse sistema de transmissão de rádio e pelo WSN (*Wireless Sensor Network*)[329].

De acordo com o relatório do conselho da Europa sobre Internet das coisas, a sociedade civil, principalmente os grupos ligados as liberdades civis, expressam preocupações sobre o limite de utilização dessas *tags*. O receio desses grupos é que o sistema de RFID se transforme em uma oportunidade de vigilância constante, por parte das empresas, das preferências de compra, de rotas e dos hábitos de consumo dos usuários. O relatório também ressalta que esse tipo de identificação do usuário encontra mais espaço em tecnologias como os carros inteligentes, em que o leitor RFID identificaria o dono do veículo, e o adaptaria de acordo com a sua comodidade[330].

Nesses sistemas de radiofrequência, as ameaças à privacidade podem ser divididas em dois grupos. O primeiro se refere à inexistência de barreira para a leitura das *tags*, tendo em vista que, em princípio, as ondas de rádio uma vez enviadas podem ser lidas por qualquer pessoa. O segundo é a sua autenticação, que é frágil (ainda que o objetivo de se ter as *tags* seja para identificação), tendo em vista que essas *tags* podem ser utilizadas como vetores de *softwares* ou *malwares* (maliciosos).[331] De acordo com o relatório da Comissão Europeia[332]:

> Um grupo da Universidade Livre de Amsterdã mostrou que RFIDs podem ser infectados por vírus que podem se espalhar através de middleware em bancos de dados onde eles podem se propagar.[333]

---

[329] MEDAGLIA, Carlo Maria; SERBANATI, Alexandru. *An Overview of Privacy and Security Issues in The Internet of Things*. Apresentado no vigésimo workshop de comunicações digitais, 2010.

[330] MILLER, Georgia e KEARNES, Matthew. *Nanotechnology, Ubiquitous Computing and The Internet of Things*: Challenges to Rights to privacy and data protection. Draft Report to the Council of Europe, set. 2013.

[331] MEDAGLIA, Carlo Maria; SERBANATI, Alexandru. "An Overview of Privacy and Security Issues in The Internet of Things", 2010, op.cit

[332] MILLER, Georgia e KEARNES, Matthew. "Nanotechnology, Ubiquitous Computing and The Internet of Things: Challenges to Rights to privacy and data protection", 2013, op.cit.

[333] Tradução livre do autor. No original: *"A group from the Free University of Amsterdam has shown that RFIDs can be infected by viruses that can spread via middle ware into databases where they can propagate."*

A baixa capacidade computacional desses dispositivos também é apontada negativamente pelos teóricos Antonio F. Skarmeta, José Ramos e Victoria Moreno, em seu artigo *"A decentralized approach for security and privacy challenges in the Internet of Things"*. Os autores ressaltam que os protocolos tradicionais e a criptografia atual demandam uma grande quantidade de memória e recursos de computador, o que dificulta a sua implementação em alguns objetos que fazem uso da tecnologia *IoT*. Para lidar com esses problemas, os autores sugerem a modificação de três aspectos nos atuais objetos com essa tecnologia[334]:

1) Criação de protocolos de segurança e algoritmos criptográficos leves;

2) Implementações leves e eficientes de protocolos de segurança e algoritmos criptográficos;

3) Implementações seguras em hardware e/ou software.[335]

A tecnologia de *"cryptographic algorithms"*, ainda que seja ideal para garantir a segurança necessária, não é capaz de prover os atributos de escala e interoperabilidade necessários para o cenário de Internet das Coisas. Por conta disso, os autores sugerem a *"public key cryptography"* (que também tem falhas por requerer desenvolvimento da memória e dos recursos de computação desses objetos).

Esses problemas fizeram com que alguns especialistas do setor concluíssem que[336]: "*sem fundações fortes, ataques e disfunções na Internet das coisas superarão qualquer um dos seus benefícios*"[337]. É bem verdade que esse tipo de tecnologia aparenta estar em um paradoxo. Ao mesmo tempo em que esses novos recursos geram benefícios e conforto ao consumidor, podem servir para lhe

[334] SKARMETA, Antonio; RAMOS José; MORENO, Victoria. *A decentralized approach for security and privacy challenges in the Internet of Things*. Apresentado no IEE World Forum, 2014.
[335] Tradução livre do autor. No original: "1) *Design of lightweight security protocols and cryptographic algorithms; 2) Lightweight and efficient implementations of security protocols and cryptographic algorithms; 3) Secure implementations in hardware and/or software*".
[336] ROMAN, Rodrigo; NAJERA, Pablo; LOPEZ, Javier. Securing the Internet of Things. *IEEE Computer*, v. 44, p. 51 -58, 2011.
[337] Tradução livre do autor. No original: "*Without Strong foundations, attacks and malfunctions in the Internet of things will outweigh any of its benefits*".

gerar danos. Esse dilema fica explícito nas palavras de Paul Ohm[338]: "*Utilidade e Privacidade são, no fundo, dois objetivos em guerra um com o outro*"[339].

Em pouco tempo provavelmente teremos nosso cotidiano monitorado, em sua grande parte, por meio dos produtos da IoT. Dessa maneira, a privacidade do consumidor é um importante tópico de discussão, pois caso os dados obtidos não sejam submetidos a um processo de proteção confiável, isso pode causar graves violações à privacidade.

Sobre essa questão, Scott R. Peppet argumenta que a política de dados é um dos aspectos que necessita de imediata reforma. Para o teórico, a exigência de consentimento dos usuários de serviços de Internet por parte do Estado e pelas empresas têm sido a principal política a ser executada quando se está a tratar sobre às informações dos consumidores desses tipos de serviços. No entanto, no cenário de IoT, a aplicação desse tipo de política encontra desafios técnicos e legais.

Um dos principais desafios técnicos apontados pelo autor remete ao fato de que muitos objetos carecem de uma interface (como uma tela ou um teclado) que possibilite ao usuário interagir com o software do objeto, conhecendo a política de tratamento de dados e consentindo com o uso de suas informações. Por conta dessa dificuldade, algumas empresas do setor optam por explicitar a política de privacidade nos seus *sites*.

A pesquisa realizada por Peppet[340] aponta, contudo, que essas políticas de privacidade enfrentam dois problemas: o da ambiguidade e o da omissão. O problema da ambiguidade se deve à indefinição do enquadramento dos dados obtidos por meio de sensores ou medição biométrica como "dados pessoais", o que consequentemente, altera a maneira como esses dados podem ser utilizados pela empresa e por terceiros. A omissão, por sua vez, deriva do fato de que algumas empresas, conforme pesquisadas por Peppet, falham no dever de informação, não cientificando o consumidor na sua política de dados sobre questões importantes, como de quem seria a posse dos dados oriundos dos sensores e sobre o tratamento dos dados. Por conta dessas questões, o autor

[338] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, v. 57, p. 43, 2010.
[339] Tradução livre do autor. No original: "*Utility and Privacy are, at bottom, two goals at war with one another*".
[340] PEPPET, Scott R. Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, v. 93, n. 85, p. 85-176, 2014.

conclui que essas políticas foram criadas para o cenário da Internet e não para o de IoT.

Antonio F. Skarmeta, José Ramos e Victoria Moreno[341] ressaltam que as fragilidades na privacidade e na segurança, no processo de armazenamento de dados, poderiam ser solucionadas caso fosse instituído um sistema de *privacy-by-design.*

O conceito de *privacy-by-design* foi desenvolvido na década de 90 por Ann Cavoukian com o intuito de alterar a forma com que a privacidade, em sistemas de dados de grande escala, era tratada. O grande objetivo desse sistema é assegurar que a garantia de privacidade seja o modo de atuação padrão das empresas. Nesse sistema, a privacidade é incorporada à própria arquitetura dos sistemas e processos desenvolvidos, de modo a garantir, pela infraestrutura do serviço prestado, condições para que o usuário seja capaz de preservar e gerenciar sua privacidade e a coleta e tratamento de seus dados pessoais.[342]

Segundo Carla Alves (et al.)[343], no conceito de *privacy by design*, a proteção da privacidade advém da seguinte trilogia: (i) sistemas de tecnologia da informação (IT *systems*); (ii) práticas negociais responsáveis (*accountable business practices*); e (iii) design físico e infraestrutura de rede (*physical and networked infrastructure*).

> O conceito em tela é fundado em sete princípios fundamentais: (i) *Proactive not Reactive; Preventative not Remedial,* pelo qual é adotada postura preventiva, de modo a evitar incidentes de violação à privacidade; (ii) *Privacy as the Default Setting*, pelo qual a configuração padrão de determinado sistema deve preservar a privacidade do usuário; (iii) *Privacy Embedded into Design*, pelo qual a privacidade deve estar incorporada à arquitetura de sistemas e modelos de negócio; (iv) *Full Functionality — Positive-Sum, not Zero-Sum*, pelo qual devem ser acomodados todos os interesses envolvidos, evitando falsas dicotomias que levam à mitigação de direitos; (v) *End-to-End Security — Full Lifecycle Protection*, vez que, na medida em que a segurança de dados é incorporada ao sistema antes da coleta de qualquer informação, esta é estendida para todo o ciclo de vida da informação; (vi) *Visibility and Transparency — Keep it Open*, pelo qual deve ser assegurado a todos os envolvidos que os sistemas sejam operacionalizados de acordo com as premissas e objetivos informados; e (vii) *Respect for User Privacy — Keep it User-Centric*, que exige que os

[341] SKARMETA, Antonio; RAMOS José; MORENO, Victoria. *A decentralized approach for security and privacy challenges in the Internet of Things*. Apresentado no IEE World Forum, 2014.
[342] Disponível em: <https://jota.info/colunas/direito-digital/direito-digital-privacy-design-e-protecao-de-dados-pessoais-06072016>. Acesso em: 27 mar. 2017.
[343] Ibid.

> operadores dos serviços respeitem os interesses dos usuários, mantendo altos padrões de privacidade.[344]

Já no sistema de *privacy by default*,[345] as configurações de privacidade mais estritas se aplicam automaticamente quando o cliente adquire um novo produto ou serviço. Em outras palavras, nenhuma mudança manual nas configurações de privacidade deve ser exigida por parte do usuário. Há também um elemento temporal para este princípio, pois as informações pessoais devem, por padrão, ser mantidas apenas pelo tempo necessário para fornecer o produto ou serviço.

As empresas desenvolvedoras de dispositivos de IoT devem ter como princípio norteador o aprimoramento da sua capacidade de assegurar a segurança e a privacidade dos usuários nos momentos de coleta, tratamento e compartilhamento de dados. As empresas podem e devem tornar este modelo de negócio mais eficiente, mas ao mesmo tempo seguro, transmitindo confiança ao consumidor e respeitando seus direitos.

Analisaremos no capítulo seguinte as regulações existentes e as possibilidades regulatórias futuras para o cenário de IoT, bem como as estratégias e novas ferramentas de proteção técnica da privacidade.

[344] Disponível em: <https://jota.info/colunas/direito-digital/direito-digital-privacy-design-e-protecao-de-dados-pessoais-06072016#_ftn6>. Acesso em: 27 mar. 2017.

[345] EU Data Protection Regulation. Data Protection by Design and by Default. *EU Data Protection Regulation*, [s.d.]. Disponível em: <http://www.eudataprotectionregulation.com/data-protection-design-by-default>. Acesso em: 31 mar. 2017.

2

O impacto da internet das coisas sob a ótica da proteção da privacidade e dos dados pessoais: a tensão entre segurança, privacidade e inovação no cenário de hiperconectividade

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

(Edward Snowden)

O cenário de Internet das Coisas (*IoT*) traz novos desafios regulatórios ao arcabouço normativo atualmente existente. Diante do contexto de constante e intenso armazenamento, tratamento, compartilhamento e monetização dos dados que trafegam online é crucial debatermos as noções de privacidade e ética que deverão nortear os avanços tecnológicos. Devemos refletir, ainda, sobre o mundo em que queremos viver e sobre como nos enxergamos nesse novo mundo de dados, decisões algorítmicas e intensificação da relação entre homens e Coisas relacionado ao novo cenário de IoT.

Em especial, com relação à privacidade[346], os dispositivos da IoT, ao coletarem uma quantidade imensa de dados referentes a incontáveis aspectos da

[346] O direito à privacidade é considerado como "tipificação dos direitos da personalidade, que são inerentes ao próprio homem e têm por objetivo resguardar a dignidade da pessoa humana. Surgem como uma reação à teoria estatal sobre o indivíduo e encontram guarida em documentos como a Declaração dos Direitos do Homem e do Cidadão, de 1789, a Declaração Universal dos Direitos do Homem, de 1948 (art. 12), a 9ª Conferência Internacional Americana de 1948 (art. 5º), a Convenção Europeia dos Direitos do Homem de 1950 (art. 8º), a Convenção Panamericana dos Direitos do Homem de 1959, a Conferência Nórdica sobre o Direito à Intimidade, de 1967, além de outros documentos internacionais. Vale ressaltar que a matéria é objeto tanto da Constituição Federal de 1988 quanto do Código Civil brasileiro de 2002 (arts. 11 ao 21), o que provocou o seu tratamento mais aprofundado e amplo pela doutrina nacional." Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 27 mar. 2017.

vida dos usuários, os coloca em um novo patamar de risco.[347] Sobretudo porque não há, no Brasil, uma lei geral de proteção de dados pessoais.[348]

A Constituição Federal de 1988 protege, de maneira esparsa, o direito à privacidade, englobando, segundo a doutrina, a proteção aos dados pessoais, tanto no meio físico como digital. A Carta Magna garante, dentre os direitos fundamentais previstos em seu artigo 5º, "a inviolabilidade da intimidade e da vida privada." No ordenamento infraconstitucional, o Código Civil, o Código de Defesa do Consumidor ("CDC") e, mais recentemente, o Marco Civil da Internet ("MCI"), disciplinaram de forma mais específica a referida proteção.

Apesar de serem interrelacionados, o conceito de privacidade não se confunde com o conceito de dados pessoais. Para as finalidades deste trabalho, utilizaremos o conceito de privacidade defendido pelo jus-filósofo italiano Stefano Rodotá, como sendo "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".[349] Defenderemos a partir deste conceito a tese de um "direito ao não rastreio", considerando esse enquadramento mais adequado à Era da hiperconectivade.

Com relação ao conceito de proteção de dados pessoais[350], utilizaremos o enquadramento teórico de Danilo Doneda que define a proteção de dados pessoais como uma garantia de caráter instrumental, derivada da tutela da privacidade, mas que não se limita por esta, fazendo referência a todo leque de garantias

[347] BRASIL. Escola Nacional de Defesa do Consumidor. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010, p. 61.

[348] A necessidade de uma lei geral de proteção dos dados pessoais se justifica pelo fato de ser especificamente voltada para coibir abusos relacionados aos dados pessoais, bem como pelo fato de trazer definições conceituais e técnicas importantes como, por exemplo, sobre "dados sensíveis".

[349] RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[350] O projeto de Lei nº 5.276 de 2016, enviado ao Congresso pelo Poder Executivo prevê, em seu art 5º, I, que *dado pessoal* é todo "*dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa"*. Portanto, dados pessoais são todos aqueles que podem identificar uma pessoa como – números, características pessoais, qualificação pessoal, dados genéticos etc. O PL também definiu alguns tipos de dados pessoais mais específicos, como os *dados sensíveis*. Tratam-se de informações que podem ser utilizadas de forma discriminatória e, portanto, carecem de proteção especial. O art. 5º, III, do PL 5.276/2016 define dados sensíveis como aqueles sobre a origem racial ou étnica de um indivíduo; suas convicções religiosas; filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político; sobre sua saúde ou vida sexual; e dados genéticos e biométricos.

fundamentais que se encontram no ordenamento brasileiro.[351] Danilo Doneda, em relatório elaborado para a Escola Nacional de Defesa do Consumidor pontua: [352]

> A proteção de dados pessoais é uma maneira indireta de atingir um objetivo último, que é a proteção da pessoa. Ao estabelecer um regime de obrigações para os responsáveis pelo tratamento de dados, bem como de direitos para os titulares destes, não se está meramente regulando um objeto externo à pessoa, porém uma representação da própria pessoa. Os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantém uma ligação concreta e viva com a pessoa titular destes dados. Os dados pessoais são a pessoa e, portanto, como tal devem ser tratados, justificando o recurso ao instrumental jurídico destinado à tutela da pessoa e afastando a utilização de um regime de livre apropriação e disposição contratual destes dados que não leve em conta seu caráter personalíssimo. Também destas suas características específicas deriva a consideração que, hoje, diversos ordenamentos jurídicos realizam, de que a proteção de dados pessoais é um direito fundamental - uma verdadeira chave para efetivar a liberdade da pessoa nos meandros da Sociedade da Informação.

Nesse sentido, devemos ter em mente que essas informações pessoais estão ligadas aos direitos da personalidade[353] dos usuários. Para protegê-las, bem como proteger a dignidade humana, é necessário assegurar a tutela dos dados pessoais. A Constituição consagrou o princípio da dignidade humana como fundamento da República, configurando cláusula geral de tutela e promoção da pessoa humana.

O conceito de dignidade da pessoa humana é difícil de ser definido, dado sua amplitude e abstração. Diversos doutrinadores brasileiros buscaram conceituar esse valor. Em definição de Ingo Sarlet[354], a dignidade da pessoa humana é algo intrínseco a cada ser humano, que – por sua condição de humanidade – se torna merecedor do respeito e consideração do Estado e dos outros seres humanos. Ainda segundo Sarlet, quando se fala em direito à dignidade, se está, em verdade,

---

[351] Vide: RODOTÁ, Stefano. (2008). *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro, Renovar. DONEDA, Danilo. (2006). *Da privacidade à proteção de dados pessoais*. Rio de Janeiro, Renovar.

[352] BRASIL. Escola Nacional de Defesa do Consumidor. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010, p. 39.

[353] BRASIL. Escola Nacional de Defesa do Consumidor. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010, p. 21. Os direitos à intimidade, à privacidade e à honra, fazem parte dos Direitos da Personalidade e estes, segundo Sílvio Venosa, "São direitos privados fundamentais, que devem ser respeitados como conteúdo mínimo para permitir a existência e a convivência dos seres humanos, (...) cabendo ao Estado reconhecê-los". Vide: VENOSA, Sílvio de Salvo. *Direito civil:* parte geral. 13. Ed. São Paulo: Atlas, 2013.

[354] SARLET, Ingo Wolfgang. *Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988*. 2001, p. 50.

a considerar o direito a reconhecimento, respeito, proteção e até mesmo promoção e desenvolvimento da dignidade, podendo inclusive falar-se de um direito a uma existência digna.[355]

Segundo Maria Celina Bodin[356], o princípio constitucional da dignidade é o único princípio capaz, na atualidade, de conferir a unidade axiológica e a lógica sistemática necessárias à recriação dos institutos jurídicos e das categorias do direito civil. Segundo Bodin, o substrato material da dignidade pode ser desdobrado em quatro postulados: i) o sujeito moral (ético) reconhece a existência dos outros como sujeitos iguais a ele; ii) merecedores do mesmo respeito à integridade psicofísica de que é titular; iii) é dotado de vontade livre, de autodeterminação; iv) é parte do grupo social, em relação ao qual tem a garantia de não vir a ser marginalizado. São corolários desta elaboração os princípios jurídicos da igualdade, da integridade física e moral — psicofísica —, da liberdade e da solidariedade.[357] Nas palavras da jurista:

> A 'dignidade da pessoa humana' decorre do reconhecimento da pessoa como um ser integrado à natureza, dotado de uma racionalidade evoluída, com a capacidade de reconhecer-se no próximo, relacionar-se com ele, exercendo sua aptidão para dialogar e amar. (...) Para Kant a "dignidade da humanidade consiste precisamente nesta capacidade de ser legislador universal, se bem que com a condição de estar ao mesmo tempo submetido a essa mesma legislação" e, por isso, "a autonomia é pois o fundamento da dignidade da natureza humana e de toda a natureza racional".
>
> Portanto, o simples fato de integrar o gênero humano, já qualifica a pessoa como destinatária do valor da dignidade. Esse atributo é inerente a todos os homens, decorrente da própria condição humana, que o torna credor de igual consideração e respeito por parte de seus semelhantes. A dignidade é composta por um conjunto de direitos existenciais compartilhados por todos os homens, em igual proporção. não obstante as diversidades sócio-culturais dos povos. A Declaração Universal dos Direitos Humanos, já em seu art. 1º, põe em destaque os dois pilares da dignidade humana: "Todas as pessoas nascem livres e iguais em dignidade e direitos. São dotadas de razão e consciência e devem agir em relação umas às outras com espírito de fraternidade." [358]

---

[355] SARLET, Ingo Wolfgang. *Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988*. 2001, p. 71.

[356] Disponível em: <https://dcivil1.blogspot.com.br/2015/09/o-principio-da-dignidade-da-pessoa.html>. Acesso em: 27 mar. 2017.

[357] CHAUI, Marilena. Convite à filosofia, op. cit., p. 338.

[358] Segundo Kant: "O homem – e, de uma maneira geral, todo o ser racional – existe como fim em si mesmo, e não apenas como meio para o uso arbitrário desta ou daquela vontade.". A dignidade constitui, na moral kantiana, um valor incondicional e incomparável. KANT, Immanuel. Fundamentação da Metafísica dos Costumes. 2003, p. 58. Disponível em: <http://www.tjrj.jus.br/c/document_library/get_file?uuid=5005d7e7-eb21-4fbb-bc4d-12affde2dbbe>. Acesso em: 27 mar. 2017.

Entretanto, pretendemos ir além desta concepção neste trabalho, tendo em vista que esta noção de 'dignidade da pessoa humana' traz subjacente uma determinada concepção da pessoa que vem sendo posta em xeque. A noção de dignidade prevista hoje pelo ordenamento jurídico usa como parâmetro o Homem dotado de razão e vontade, elementos que o distingue dos demais seres vivos, colocando-o num patamar superior. Do ponto de vista ontológico, a concepção de pessoa humana baseia-se em uma perspectiva dualista: homem vs natureza ou homem vs coisa, que estariam níveis diversos, respectivamente sujeito e objeto.

Segundo o próprio Sarlet:[359]

> "(...) tanto o pensamento de Kant quanto todas as concepções que sustentam ser a dignidade atributo exclusivo da pessoa humana – encontram-se, ao menos em tese, sujeitas à crítica de um excessivo antropocentrismo, notadamente naquilo em que sustentam que a pessoa humana, em função de sua racionalidade, ocupa lugar privilegiado em relação aos demais seres vivos. "

Reforçando essa leitura crítica, o professor da UFBA Marco Aurélio Castro Júnior,[360] reconhece que o paradigma fundamental do Direito atual é o antropocentrismo e que o crescente avanço tecnológico abre as portas para a criação de Coisas potencialmente mais inteligentes que os humanos, o que poderá ser determinante para a decadência do antropocentrismo. Nas palavras de Castro:

> É lícito afirmar que se outro ente for encontrado dotado desses mesmos elementos a conclusão lógica é a de se lhe atribuir o mesmo status jurídico de pessoa. (...) Hoje as legislações vigentes em Portugal e no Brasil aboliram adjetivos dos seus conceitos de pessoa, abrindo a porta para que se compreenda como pessoa, como dotado de personalidade jurídica, não apenas o Homem, mas à moda da visão oriental sobre a equiparação da dignidade de todos os seres com o Homem, dando chances à teoria do direito animal e, assim, também a do direito robótico para que um robô seja juridicamente qualificado como Pessoa".

Por conta desta problemática, buscaremos neste trabalho melhores enquadramentos regulatórios e conceituais em relação à privacidade e à proteção dos dados pessoais, bem como analisaremos o avanço das Coisas inteligentes cada vez mais autônomas e simbióticas às relações sociais. Sob essa ótica, poderemos compreender melhor o grau de influência que mecanismos não-humanos podem

[359] SARLET, Ingo Wolfgang. *Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988*. 4. ed. Porto Alegre: Livraria do Advogado, 2006.
[360] CASTRO, Marco Aurélio. *Personalidade jurídica do robô e sua efetividade*. Salvador: 2009.

exercer sobre a vida em sociedade e a importância dos seus efeitos, inclusive sobre a esfera pública.[361]

Por conta da quantidade de atores, artefatos e temas envolvidos, a Internet das Coisas exigirá uma nova governança[362], e muitos são os interessados em influenciar a regulação do tema. Tendo em vista que o mercado de IoT conjuga a necessidade de assegurar um custo competitivo e um baixo custo para alcançar o mercado de massa, estes fatores, aliados ao ritmo de produção de novos produtos, faz com que os dispositivos não tenham muitas vezes as credenciais de segurança e privacidade necessárias. [363] Por isso, privacidade e segurança são tidas como duas das questões mais importantes da IoT. [364]

É importante também examinarmos essas regulações sob o ponto de vista do impacto no fomento de inovações tecnológicas, uma vez que não seria benéfico para a sociedade que as leis existentes trouxessem disposições extremamente rígidas que impedissem o desenvolvimento tecnológico e a inovação. Assim, é preciso assegurar a proteção dos usuários da Internet das Coisas, mas deixar espaço aberto para que a tecnologia possa continuar a ser aperfeiçoada. Nesse sentido, Marcel Leonardi considera que: "Ao restringir, regulamentar, com base nos piores casos, pode-se não deixar florescer os melhores casos. (...) O modelo que temos de ter é uma regulação *ex post* com regulação dos abusos"[365].

Por outro lado, afirma Manuel Estrada:

> A IoT captura dados a cada minuto em que andamos na rua, estacionamos os nossos carros ou cada vez que usamos um smartphone ou cartão de crédito. À medida que é recolhida cada vez mais informações pessoais, surgem preocupações relativamente aos perfis, discriminação, exclusão, vigilância do governo e perda de controle. Os avanços tecnológicos já ultrapassaram

[361] Para isso, as correntos de pós-humanismo e pós-estruturalismo nos ajudarão a compreender as novas características da contemporaneidade, considerando os poderes de agência desses elementos não-humanos, e fornecendo meios para interpretar a sua atuação.
[362] CHAVES, Luis Fernando Prado; GOMES, Maria Cecilia Oliveira. Por que a Internet das Coisas revolucionará o Direito Digital? *Justificando*, 20 fev. 2017. Disponível em: <http://justificando.cartacapital.com.br/2017/02/20/por-que-Internet-das-coisas-revolucionara-o-direito-digital/>. Acesso em: 21 fev. 2017.
[363] HERNANDEZ, Leandro. Desafio da 'Internet das coisas' é impedir quebra de privacidade. *Notícias Uol*, 2015. Disponível em: <https://noticias.uol.com.br/opiniao/coluna/2015/07/18/desafio-da-Internet-das-coisas-e-impedir-quebra-de-privacidade.htm>. Acesso em: 21 fev. 2017.
[364] PRESCOTT, Roberta. Internet das coisas demanda boas práticas e não regulação prévia. *Associação Brasileira de Internet*, 2015. Disponível em: <http://www.abranet.org.br/Noticias/Internet-das-coisas-demanda-boas-praticas-e-nao-regulacao-previa-830.html#.WKyJFG8rLct>. Acesso em: 21 fev. 2016.
[365] Ibid.

> claramente os quadros legais existentes, criando uma tensão entre inovação e privacidade, sempre que as leis não refletem os novos contextos sociais e não garantem os direitos dos cidadãos.[366]

Enquanto não há legislação específica tratando da IoT é preciso analisar, em primeiro lugar, os diplomas vigentes que podem ter aplicação neste setor[367] - sobretudo o CDC e o Marco Civil da Internet. Veremos a partir de agora, portanto, as regulações existentes e aplicáveis, dispostas em ordem cronológica, bem como as novas propostas regulatórias para essa área.

2.1
A Regulação do Código de Defesa do Consumidor (CDC) e a IoT

O Código de Defesa do Consumidor (CDC) possui dispositivos que buscam assegurar a privacidade e a segurança dos consumidores, parte vulnerável na relação consumerista.

Quanto à segurança, o CDC elege como princípio da Política Nacional das Relações de Consumo, no artigo 4º, II, d, ação governamental no sentido de proteger o consumidor "pela garantia dos produtos e serviços com padrões adequados de qualidade, segurança, durabilidade e desempenho." Ou seja, o governo não só está autorizado a intervir para proteger o consumidor, como tem o dever fazê-lo. Esta é uma medida positiva do ponto de vista do consumidor, já que responsabiliza diretamente o fabricante quando da ocorrência de algum dano, porém mecanismos repressivos devem ser vistos com cautela para não acabarem tornando-se um óbice ao processo criativo das indústrias, ainda mais diante de um contexto no qual o conhecimento geral sobre tais produtos ainda está caminhando.

Em seguida, dispõe no inciso II do art. 6º, "a educação e divulgação sobre o consumo adequado dos produtos e serviços", o que terá grande aplicabilidade à

[366] ESTRADA, Manuel Martín Pino. O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade. *Revista de Direito do Trabalho*, v. 172, p. 43, nov./dez. 2016.

[367] O Brasil possui dezenas de leis que, direta ou indiretamente, tratam do tema proteção de dados. Desde o Marco Civil da Internet e seu decreto regulamentador, que trazem regras rígidas e aplicáveis a todos os serviços de Internet e o Código de Defesa do Consumidor, até leis ainda mais específicas como a Lei do Cadastro Positivo, a Lei do E-Commerce e a Lei do Sigilo Bancário. Para os fins deste trabalho restringiremos nossa análise ao M.C.I. e ao C.D.C., além do C.C. e da C.F. em função de relevância ser mais abrangente que os demais diplomas de menor escopo.

Internet das Coisas. É preciso informar aos usuários sobre os possíveis riscos que podem vir a se concretizar com o uso dos dispositivos e sobre as informações que serão coletadas com tal uso. Os inúmeros dispositivos de IoT conectados à Internet, põem em cheque os direitos de "proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos", previstos no inciso I do artigo 6º do CDC.

O risco advindo de tais dispositivos se agrava ainda pelo fato de que indústrias ligadas ao desenvolvimento de dispositivos analógicos - não especializadas na tecnologia digital, portanto - passam agora a criar objetos de *IoT*, muitas vezes sem dar atenção ou sem expertise em segurança e privacidade em IoT. [368]. Do ponto de vista dessas indústrias, aproveitar a visibilidade crescente dos produtos conectados *online* a fim de obter lucro imediato pode ser mais importante do que preocupar-se com possíveis defeitos ou riscos à privacidade. O mercado usualmente age dessa forma, o que vai de encontro a toda a ideia-base do CDC[369]. Nesse sentido, confira-se o que pontuou o Instituto Brasileiro de Defesa do Consumidor, com base em relatório do *Federal Trade Comission* (FTC):

> Há um problema grave quando fornecedores de produtos e serviços da "indústria off-line" passam a fazer parte da cadeia de produtores de tecnologias de conexão à Internet, sem expertise técnica e sem os cuidados dos profissionais de segurança da informação, tipicamente ligados ao universo da computação, da T.I. e do gerenciamento de redes. Esse movimento da indústria exige atenção e atuação regulatória para evitar lesão aos consumidores.[370]

Nas palavras de Bruno Miragem, ao dissertar sobre a Internet das Coisas e os riscos do que considera um admirável mundo novo:[371]

> Esse estado de coisas resulta na própria reavaliação da extensão do dever de segurança dos produtos e serviços no mercado de consumo. A legislação brasileira é expressa ao limitar o fornecedor, indicando que coloque no mercado

[368] ZANATTA, Rafael A. F. Internet das Coisas: privacidade e segurança na perspectiva dos consumidores [Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017] – *Instituto Brasileiro de Defesa do Consumidor*, 2017.

[369] Daí a importância do engajamento da coletividade na busca de informação não apenas sobre como utilizar os produtos, mas sobre o quanto as empresas têm levado em conta a proteção da privacidade e segurança ao elaborarem seus produtos, ideia corroborada pelo legislador ao definir como direito básico do consumidor a educação e divulgação sobre o consumo de produtos (conforme inciso II do artigo 6º do Código de Defesa do Consumidor).

[370] ZANATTA, Rafael A. F. 2017, op.cit.

[371] Disponível em: <http://www.conjur.com.br/2017-mar-29/garantias-consumo-Internet-coisas-riscos-admiravel-mundo>. Acesso em: 27 mar. 2017.

> apenas produtos cujos riscos sejam normais e previsíveis (artigo 8º do CDC). A pergunta óbvia aqui será: todos os riscos destas novas tecnologias serão normais e previsíveis? Ou mesmo, em vista da cláusula geral de responsabilidade objetiva fundada no risco, prevista no artigo 927, parágrafo único, do Código Civil, de que modo seria identificada "a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem"? As implicações jurídicas da Internet das coisas não param, contudo, por aí. Basta imaginar sua repercussão para o sistema de seguros e a avaliação dos riscos segurados, mesmo para permitir a definição de cobertura e de seu custo para o segurado (assim, o seguro de danos de um automóvel sem motorista, ou o seguro de vida de um segurado cujas informações de saúde sejam monitoradas em tempo real).

É importante assinalar, conforme dito anteriormente, que os produtos de IoT irão falhar e isso é esperado. É, ainda, preferível que eles falhem o quanto antes para que sejam reparados em tempo de não gerarem maiores danos, além de incetivar a corrida industrial por aperfeiçoamento dos dispositivos. No entanto, é de suma importância que a indústria faça o maior esforço técnico possível de enviá-lo ao mercado como produto adequado à utilização da coletividade, ou seja, somente após passar por uma robusta fase de testes que reduzam o escopo de imprevistos.

Nesse sentido, a leitura do CDC deve ser feita através de uma interpretação extensiva, diferenciando riscos "inerentes" daqueles completamente inesperados, pois se um alarde for criado em volta dos produtos conectados *online*, há o risco sério de inibir inovações e espalhar na sociedade uma onda irracional de receio quanto ao real objetivo técnico destes.

Em alguns dispositivos da IoT, como lâmpadas e fechaduras, são inseridos minicomputadores, que não possuem a capacidade de segurança e de lidar com antivírus como um computador normal. Quanto a tais riscos de segurança, Eduardo Prado pontua:

> As margens de lucro desses pequenos computadores são muito limitadas e, por isso, os fabricantes têm pouco espaço para gastos com segurança. E os sistemas estão sendo produzidos em grandes quantidades, de forma que se os hackers encontrarem uma falha em um deles, será possível entrar em muitos outros também. Para piorar as coisas, a HP anunciou recentemente um estudo que indica que 70% dos dispositivos mais comuns de IoT exibem sérias vulnerabilidades que podem ser exploradas pelos hackers.[372]

[372] PRADO, Eduardo. Internet das Coisas vai obrigar mudanças no Marco Civil da Internet. *Convergência Digital*, 2014. Disponível em: <http://sis-publique.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=37768&sid=15>. Acesso em: 27 mar. 2017.

Corroborando com essas preocupações levantadas, recentemente na Alemanha, por exemplo, uma boneca interativa chamada "My Friend Cayla" foi proibida pelo governo alemão, por conter um "dispositivo de vigilância ilegal".[373] O brinquedo possuía um microfone Bluetooth-conectado que emulava a voz de uma criança.

Nos Estados Unidos, vários grupos de proteção ao consumidor se uniram para registrar uma queixa à FTC não somente contra a boneca Cayla mas também contra um "robô inteligente" denominado i-Que também fabricado pela Genesis Toys.

Levantou-se que a Cayla mantinha conversas com as crianças pedindo-lhes informações como os nomes de seus pais, as escolas onde estudavam e seu endereço de residência.[374] Verificou-se nas investigações que o arquivo de áudio e as transcrições de texto armazenadas pela boneca poderiam ser vendidos para agências militares, de inteligência e de aplicação da lei.

Além disso, qualquer um que ligasse para um dos telefones pareados automaticamente poderia conversar com a criança através do brinquedo. Hackers também conseguiriam programar as bonecas para ignorar as proteções contra o uso de linguagem inapropriada, dando novos inputs comunicativos e usando a boneca como meio para introduzir diretamente para as crianças propagandas não desejadas pelos pais.[375]

> A boneca My Friend Cayla com conexão Bluetooth, é comercializada como um "amigo com quem você pode conversar" através do seu microfone embutido. Mas, novamente, é uma rua de dois sentidos. Indivíduos desonestos poderiam *hackear* a boneca para supervisionar crianças e falar com elas de forma clandestina. A boneca Cayla foi banida na Alemanha, declarada como um "brinquedo proibido". Os pais que já compraram o brinquedo foram convidados a destruí-los, e a nova proibição prevê fortes multas e prisões. O Conselho Norueguês do Consumidor designou a Cayla como um brinquedo falido que viola as leis europeias de privacidade dos consumidores. A empresa nega que o brinquedo seja inseguro. A boneca Cayla ainda está disponível nos Estados Unidos.[376]

---

[373] Disponível em: <https://www.nexojornal.com.br/expresso/2017/02/23/Qual-%C3%A9-o-problema-e-o-debate-por-tr%C3%A1s-da-boneca-espi%C3%A3>. Acesso em: 27 mar. 2017.

[374] Disponível em: <http://www.telegraph.co.uk/news/2017/02/17/germany-bans-internet-connected-dolls-fears-hackers-could-target/>. Acesso em: 27 mar. 2017.

[375] Disponível em: <https://www.nexojornal.com.br/expresso/2017/02/23/Qual-%C3%A9-o-problema-e-o-debate-por-tr%C3%A1s-da-boneca-espi%C3%A3>. Acesso em: 27 mar. 2017.

[376] Tradução livre do autor. No original: *The Bluetooth-connected My Friend Cayla doll is marketed as a "friend you can talk with" via its embedded microphone. But again, it's a two-way*

Na avaliação das autoridades reguladoras do governo alemão, Cayla não é confiável. O comunicado afirma que "itens que tenham câmeras ou microfones, e que sejam capazes de transmitir sinais e, portanto, transmitir dados sem conhecimento do dono, comprometem a privacidade das pessoas". Por isso, o brinquedo de IoT Cayla foi banido da Alemanha.[377]

Assim, o investimento das empresas em segurança e privacidade no desenvolvimento dos novos produtos de IoT bem como a consciência crítica dos consumidores sobre esses riscos, passam a ser fundamentais e colocam muitas vezes nossas previsões legais em questionamento.[378]

---

street. Dodgy characters could hack the doll to surveil children and clandestinely speak to them. The Cayla doll has been banned in Germany and declared a "forbidden toy." Parents who already bought the toy have been asked to destroy them, and the new ban calls for hefty fines and jail terms. The Norwegian Consumer Council has designated Cayla as a failed toy that violates European consumer privacy laws. The company denies the toy is unsafe, and the Cayla doll is still available in the United States. Disponível em: <https://www.noozhawk.com/article/diane_dimond_toys_that_can_spy_put_the_fear_in_christmas_or_should_20171216>. Acesso em: 27 mar. 2017.

[377] Disponível em: <https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children>. Acesso em: 27 mar. 2017.

[378] Essa discussão se relaciona com o conceito de "risco do desenvolvimento". Os riscos do desenvolvimento podem ser definidos como "aqueles não cognoscíveis pelo mais avançado estado da ciência e da técnica no momento da introdução do produto no mercado de consumo e que só vêm a ser descobertos após um período de uso do produto em decorrência do avanço dos estudos científicos". A questão que se coloca é que se nem mesmo o fabricante tem condições de prever os efeitos nefastos, que condições teria o consumidor/usuário de ponderar sobre as consequências do uso de um produto? Além disso, segundo Tula Wesendonck, "os fabricantes lucram com a atividade que exercem e por consequência, é bem provável que estejam mais preparados para suportar os prejuízos decorrentes dos danos que os seus produtos possam causar à sociedade, seja sob o âmbito da contratação de seguros para indenização seja pela distribuição do prejuízo no custo do produto. Esse raciocínio pode servir como um incentivo na preocupação constante de o fabricante somente colocar em circulação produtos que sejam seguros." Vale ainda mencionar a aplicação da "teoria do risco do negócio", acolhida pelo atual CDC (arts. 12 e 14), segundo a qual o fornecedor responde independentemente de culpa (responsabilidade civil objetiva) por qualquer dano causado ao consumidor, pois que, pela teoria do risco, este deve assumir o dano em razão da atividade que realiza. Segundo Pablo Dorneles, se valendo dos ensinamentos de Sergio Cavalieri: "Portanto, a intenção subjetiva pouco importa quando enfrentamos questões que envolvem relações de consumo, pois esta não faz parte dos critérios determinantes no momento de se condenar à reparação do dano, pois que, havendo ou não a pretensão de lesar, o que interessa é apenas a existência do prejuízo, e por isso, o causador é obrigado a repará-lo." TULA, Wesendonck. A responsabilidade civil pelos riscos do desenvolvimento: evolução histórica e disciplina no Direito Comparado. Direito & Justiça v. 38, n. 2, p. 213-227, jul./dez. 2012. CALIXTO, Marcelo Junqueira. O art. 931 do Código Civil de 2002 e os riscos do desenvolvimento. *Revista Trimestral de Direito Civil*, Rio de Janeiro, Padma v. 6, n. 21, p. 75-77, jan./mar. 2005. SILVA, João Calvão da. *A responsabilidade civil do produtor*, p. 75. DORNELES, Pablo. A Responsabilidade Civil Objetiva Prevista no CDC. Disponível em: < http://www.dalagnol.com.br/site.php?acao=ler&menu=artigo&codArtigo=3>. Acesso em: 27 mar. 2017.

É importante termos em mente que todas essas tecnologias atreladas à IoT possuem vulnerabilidades.[379] No entanto, considerando que esses dispositivos estão cada vez mais complexos, inclusive com maior autonomia e comportamento imprevisível, isso demanda maior responsabilidade dos desenvolvedores na produção destes artefatos e maior atenção à fase de teste controlado antes que sejam destinados à comercialização. Trataremos de forma mais aprofundada deste assunto no capítulo seguinte.[380]

Tentando coibir uma conduta displicente por parte dos fornecedores, o art. 10, caput, do CDC dispõe "o fornecedor não poderá colocar no mercado de consumo produto ou serviço que sabe ou deveria saber apresentar alto grau de nocividade ou periculosidade à saúde ou segurança". É certo que muitas vezes as empresas sequer são capazes de assegurar isto, pois como já foi dito, não empregam o esforço técnico necessário na elaboração dos produtos, porém há casos em que pode ser considerado previsível determinadas funções do produto extrapolarem sua finalidade. Exemplo disto é o Amazon Echo, alto-falante capaz de programar diferentes tarefas, além de executar audiobooks e música, através do comando de voz. O dispositivo responde pelo nome de Alexa, que se comunica com o usuário atendendo seus comandos, assim como ocorre com *Smart Tvs*, mencionadas anteriormente.

Ocorre que o sistema do Amazon Echo é ativado pela palavra "acordar", e para isto ele precisa monitorar o que está sendo dito no ambiente a fim de identificar o comando. Com isto não é difícil afirmar que o dispositivo grava vozes permanentemente, de modo que uma função específica e inerente ao seu funcionamento acaba levando a uma violação direta de privacidade e segurança dos usuários, considerando que este pode ser hackeado. Ciente disto, teoricamente a indústria não deveria fornecer um produto com tal capacidade, porém se isto ocorrer após a introdução do mesmo no mercado, o CDC prevê no parágrafo único, que o fato deve ser imediatamente comunicado às autoridades.

---

[379] Disponível em: <http://www.bbc.com/news/world-europe-39002142>. Acesso em: 27 mar. 2017.

[380] É importante termos consciência de que a tecnologia nunca é infalível. Nesse sentido, muitos designers são adeptos da teoria de que "quanto antes ela falhar, mais rápido se consegue consertar e aprimorar a Coisa (artefato técnico)". Essa é a filosofia, por exemplo, do Netflix que possue o sistema Chaos Monkey que expõe os engenheiros a falhas aleatórias e com muito mais freqüência para incentivá-los a criar serviços mais resilientes.

Na mesma esteira, o artigo 12 responsabiliza objetivamente o fabricante, produtor ou construtor por defeitos decorrentes do produto ou de seu projeto e avança no artigo 14, responsabilizando também o fornecedor. Isto significa que caso produtos de IoT apresentem alteração na funcionalidade que lhe era esperada, seus responsáveis tem o dever de reparar o dano e/ou até mesmo indenizar o consumidor.

Exemplo de mal funcionamento ou defeito de produto com tecnologia IoT, é do *Nest Thermostat*, um termostato inteligente da Amazon, que promote se adaptar às atividades dos usuários dentro de casa, bem como ao clima externo, além de favorecer a economia de energia. No entanto, há relato de usuários[381] que tiveram problemas com o funcionamento do produto, que não respondia a comandos manuais, impedindo o ajuste de temperatura por parte do usuário. Assim, a casa ficaria fria ou quente demais até que o sistema do termostato decidisse mudar a temperatura. Além disso, o aparelho não "aprende com os hábitos do usuário", conforme prometido, e poderia acabar causando danos à saúde ou constrangimentos ao consumidor, situação que ensejaria reparação pela empresa, segundo o CDC brasileiro.

Situações como essa - de frustração com o funcionamento de produtos inteligentes -, podem trazer um efeito indesejável às inovações tecnológicas. Ocorreu recentemente o caso do hotel Romantik Seehotel Jaegerwirt, na Áustria[382], no qual o Sistema de chaves eletrônicas dos quartos dos hóspedes foi hackeado e a administração do hotel decidiu por retirar todo o sistema e voltar para o mecanismo analógico. Ou seja, quando o usuário se frustra com o funcionamento do produto, ou este se mostra um risco à segurança, todo um conjunto de serviços é colocado em dúvida, e as pessoas tendem a voltar sua confiabilidade aos produtos *offline*, o que não é interessante para o fomento de tecnologia.

Outro problema dentro do campo das relações de consumo diz respeito à publicidade comportamental diante das possibilidades da IoT e sua relação com a

[381] A consumidora Kara Pernice escreveu um artigo narrando sua experiência com o *Nest Thermostat*, no qual detalha as disfunções apresentadas pelo produto ao longo do tempo. Disponível em: < https://www.nngroup.com/articles/emotional-design-fail/>. Acesso em: 27 mar. 2017.

[382] Disponível em: <https://exame.abril.com.br/tecnologia/hackers-trancam-hospedes-em-hotel-e-exigem-resgate-em-bitcoin/>. Acesso em: 27 mar. 2017.

proteção da privacidade e dos dados pessoais. Muitas vezes, os dados dos consumidores são colhidos a fim de se criar um perfil comportamental para que a publicidade seja direcionada baseada na forma como determinado consumidor age quando realiza compras. O fornecedor de produtos tem, assim, a possibilidade de ter informações individualizadas sobre os consumidores permitindo a ele guiar o fluxo informacional e a publicidade de forma particular para cada um.

Na Seção VI, o CDC trata especificamente da privacidade sob a ótica da proteção dos bancos de dados e cadastros dos consumidores. O Código assegura no artigo 43 o acesso do consumidor às informações existentes em cadastros, fichas e registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes e garante a possibilidade de o consumidor alterar os dados caso haja incorreção.

Complementarmente, quando a prática de publicidade direcionada leva ao envio de mensagens indesejadas, há uma resposta direta do CDC. O artigo 6º, inciso IV, determina como direito básico a proteção do consumidor contra "publicidade enganosa e abusiva", o que se aplica à publicidade direcionada uma vez que esta é elaborada a partir de artifícios dos quais o consumidor não tem conhecimento. Já o inciso III do artigo 39 do CDC veda ao fornecedor de produtos e serviços, dentre outras práticas abusivas, "enviar ou entregar ao consumidor, sem solicitação prévia, qualquer produto, ou fornecer qualquer serviço."

A publicidade comportamental é capaz de aumentar a assimetria de informação na relação de consumo, potencializar a discriminação entre os consumidores, minimizar a capacidade de escolha livre e autônoma do consumidor, dentre outras consequências[383].

Segundo relatório do McAfee Labs acerca de previsões sobre ameaças na Internet em 2017, a privacidade dos consumidores será reduzida de forma significativa com o desenvolvimento da IoT:

> Relatos sobre o fim da privacidade foram exagerados no passado, mas a IoT vai tornar esse fim mais próximo. Existem simplesmente dispositivos IoT demais observando, ouvindo, gravando, acumulando e acompanhando de outras formas o

[383] BRASIL. Escola Nacional de Defesa do Consumidor. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010, p. 59 e ss.

> comportamento do consumidor. Em muitos casos, os consumidores pagam a uma empresa por um serviço e se permitem ser rastreados gratuitamente. É verdade que os detalhes estão nos contratos de licença de usuário, mas a maioria dos consumidores não os lê e não consegue evitá-los, de qualquer forma. Os dispositivos IoT estão ultrapassando rapidamente os limites das atuais leis de privacidade e as instituições políticas continuarão a reagir lentamente. As expectativas de privacidade afetarão fornecedores de dispositivos e operadores de serviços, pois alguns governos exigirão contratos explícitos, adesões e até mesmo compensações pelo uso ou compartilhamento dos dados de alguém.[384]

Outro ponto importante a ser considerado é que, com o aumento da conectividade e da geração de dados pessoais, a IoT tem o potencial de aumentar o desequilíbrio de poder entre os consumidores e as empresas.[385]. Tal desequilíbrio de poder demonstra que atenção especial deve ser dada à relação entre IoT e o Código de Defesa do Consumidor. Nada obstante a provável necessidade de atualização do CDC - ou a criação de uma regulação específica para a IoT -, seus atuais dispositivos possuem aplicação à Internet das Coisas, como visto até aqui.

Diante deste cenário, é preciso observar as previsões do CDC e do Marco Civil da Internet no cenário da Internet das Coisas. A privacidade e a segurança dos usuários devem ser tuteladas ao mesmo tempo em que a normatividade deve deixar aberto o espaço para a inovação tecnológica. O artigo 4º, III, demonstra essa preocupação por parte do legislador ao prever de forma clara a "harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica".

Apesar de todas as previsões do Marco Civil da Internet e do Código de Defesa do Consumidor que visam tutelar a privacidade e a segurança dos usuários da Internet, os dispositivos existentes não são suficientes para garantir a integralidade dos direitos dos usuários de dispositivos da Internet das Coisas.

Conforme nos ensina Bruno Miragem: [386]

---

[384] MCAFEE LABS. *Previsões sobre ameaças em 2017*. nov. 2016, p. 22. Disponível em: <https://www.mcafee.com/br/resources/reports/rp-threats-predictions-2017.pdf>. Acesso em: 24 fev. 2017.

[385] ESTRADA, Manuel Martín Pino. O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade. *Revista de Direito do Trabalho*, v. 172, p. 42, nov./dez. 2016.

[386] Miragem, Bruno. A internet das coisas e os riscos do admirável mundo novo. Conjur. 2017.

> O modo como o Direito deverá enfrentar os desafios abertos pela Internet das Coisas é uma via a ser ainda percorrida. Na falta desses instrumentos, é impostergável que as situações que envolvam já essas novas tecnologias devem encontrar no jurista a prudência necessária para bem aplicar o Direito posto em soluções que equilibrem o desenvolvimento tecnológico e a liberdade da ciência, com a proteção da pessoa humana em relação aos novos riscos da vida comunitária.

De fato, determinados aspectos e cenários ligados ao desenvolvimento tecnológico devem ser deixados em aberto para que haja espaço para a inovação. Porém há casos, conforme exploraremos a seguir, em que a lei deve ter aplicabilidade para fins de coibir abusos e reparar danos ao consumidor. Assim como analisamos as possibilidades de aplicabilidade do CDC, veremos agora as possíveis conexões entre o Marco Civil da Internet e a IoT.

2.2
A Regulamentação do Marco Civil da Internet (MCI) E A IoT

O Marco Civil da Internet (Lei 12.965/2014 - "MCI")[387] aprovado em 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Na época, levando em conta os ordenamentos jurídicos e as experiências dos europeus e norte-americanos no que diz respeito à internet, restava claro que a ausência de disposições sobre direitos fundamentais básicos como a liberdade de expressão, o acesso ao conhecimento e o direito à privacidade dificultavam a aplicação da legislação em vigor e geravam inúmeras decisões judiciais conflitantes para as mais diversas controvérsias envolvendo o uso da Internet.[388][389]

Entendia-se que o debate sobre a aplicação dos direitos fundamentais na rede era prioritário e deveria preceder a discussão, por exemplo, sobre criminalização, mantendo a previsão penal como último remédio para conduzir a ordenação das condutas sociais. Nesse contexto, a reação popular após a

---

[387] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 mar. 2017.

[388] MAGRANI, Eduardo. Democracia Conectada - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.

[389] SOUZA, Carlos Affonso, FRANCISCO, Pedro, MACIEL, Marília. op. cit., p. 118.

proposição do PL número 84/99[390], lei punitiva, foi extremamente negativa. A mobilização foi tamanha, que se abriu espaço para o surgimento de uma lei civil para regulamentar a internet, nascendo assim, o Marco Civil.

Desta forma, a iniciativa teve como base consultas públicas através de uma plataforma online, abrangendo inúmeras perspectivas e opiniões de diversas instituições públicas e privadas, contando ainda com opiniões substanciais da academia e da sociedade civil. Segundo trabalho realizado pelo autor desta tese:[391]

> A empreitada foi considerada uma experiência democrática pioneira no Brasil. Foi a primeira vez que um anteprojeto de lei foi construído através de consulta pública na internet, e a maturação da discussão feita aproveitando-se do potencial das plataformas digitais na esfera pública conectada. Conjuntamente, todas as iniciativas e fases que compuseram a elaboração do anteprojeto serviram ao ideal de se estimular o debate em um ambiente em que todos tivessem a mesma chance de falar, de ouvir e de contestar, livres de influência político-econômica, visando uma maior legitimidade do anteprojeto.[392]

O MCI se pretendeu como a "Constituição da Internet" no Brasil e salvaguardou diversos princípios e direitos fundamentais. A proteção à privacidade é expressamente prevista pelo Marco Civil da Internet representando um grande avanço face ao cenário anterior ao diploma, pois o acesso aos dados e os registros das condutas dos usuários não tinham regulação específica, o que levava a uma quantidade maior de abusos e violações de direitos[393].

O Marco Civil tem como um de seus principais objetivos o apoio às inovações e novas tecnologias (Artigo 4º inciso III). Sendo assim, inventos como objetos da IoT são acolhidos pela lei. No entanto, o MCI enfrenta desafios diante do cenário de IoT. Por exemplo, uma interpretação rígida do diploma é capaz de impedir que o país tenha inovações tecnológicas e seu procedimento de coleta de dados pessoais "pode estar incoerente com o mundo da Internet das Coisas"[394],

[390] Também conhecida como Lei Azeredo pelo fato do congressista Eduardo Azeredo ter sido o relator da proposta. Para mais informações sobre esse PL e seu contexto, vide: MAGRANI, Eduardo. "Democracia Conectada...". 2014, op.cit.
[391] MAGRANI, Eduardo. "Democracia Conectada...". 2014, op.cit.
[392] Ibid.
[393] FORTES, Vinicius Borges. *Os direitos de privacidade e a proteção de dados pessoais na Internet*. Rio de Janeiro: Lumen Juris, 2016, p. 120.
[394] MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO. Marco Civil da Internet pode impedir acesso à inovação e geração de emprego, diz secretário. *Ministério da Ciência, Tecnologia e Inovação*, 2016. Disponível em: <http://www.mcti.gov.br/noticia/-/asset_publisher/epbV0pr6eIS0/content/marco-civil-da-Internet-pode-impedir-acesso-a-inovacao-e-geracao-de-emprego-diz-secretario>. Acesso em: 21 fev. 2017.

como afirmou Maximiliano Martinhão, Presidente da Telebrás e ex-secretário de Política de Informática do Ministério da Ciência, Tecnologia, Inovações e Comunicações.[395]

Ao lado da liberdade de expressão, o direito à privacidade é previsto no MCI como condição para o pleno exercício do direito de acesso à Internet (art. 8º).[396] O diploma elenca, no inciso II do artigo 3º, a proteção à privacidade como princípio a ser observado na disciplina da Internet, assim como o é a proteção de dados, prevista no inciso III.

O artigo 7º do MCI[397] possui extrema importância primeiramente pelo fato de considerar o acesso à Internet como essencial ao exercício da cidadania, em

[395] MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.

[396] Art. 8º: A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

[397] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
V - manutenção da qualidade contratada da conexão à internet;
VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

sintonia com o relatório da ONU[398] que definiu em 2011 o acesso à Rede como um direito humano. Além disso, o mesmo artigo assegura inúmeros direitos aos usuários da Internet no Brasil e tutela expressamente a privacidade em suas mais diferentes facetas.

Neste sentido, garante-se, por exemplo, a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação" (inciso I), a inviolabilidade e o sigilo de comunicações pela Internet (inciso II) e das comunicações privadas armazenadas (inciso III), exceto por ordem judicial.

Também os dados pessoais são protegidos, como prevê o inciso VII, ao positivar o direito ao "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, **salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei**" (grifos nossos). Prevê-se, ainda, o direito a informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção dos dados e suas finalidades (inciso VIII) e o **consentimento sobre a coleta e o uso dos dados** (inciso IX) (grifos nossos).

A proteção aos dados pessoais é tratada de forma específica na Seção II da Lei, cabendo destacar o que prevê o artigo 10:[399]

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, **mediante ordem judicial**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado **mediante ordem judicial**, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem **qualificação pessoal, filiação e endereço**, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

[398] Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/06/onu-afirma-que-acesso-internet-e-um-direito-humano.html>. Acesso em: 27 mar. 2017.
[399] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 mar. 2017.

> § 4º As medidas e os procedimentos de segurança e de sigilo **devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais**. (destacamos)

Sobre a guarda de registros de conexão, o art. 13, caput, do MCI prevê como dever dos provedores de conexão mantê-los em sigilo e segurança pelo prazo de 1 ano, prorrogável a pedido do Ministério Público. Já os provedores de aplicações de internet constituídos em forma de pessoa jurídica, deverão armazenar os registros de acesso sob as mesmas condições, mas pelo período de 6 meses, segundo o artigo 15. Em qualquer hipótese, a disponibilização ao requerente dos registros de que tratam estes dispositivos deverá ser precedida de autorização judicial.

Apesar destas previsões, Juliano Madalena afirma que ainda há riscos de violação da privacidade por conta da não proteção da conexão entre servidor e usuário. Apenas por meio de criptografia e demais ferramentas de anonimização haveria, segundo o autor, maior segurança de forma que somente pessoas autorizadas, como previsto no inciso II do art. 7º, teriam acesso aos dados. Confira-se o que leciona o autor: [400]

> As conexões entre os usuários ou destes com os servidores em sua natureza não são protegidas. É dizer que os dados, via de regra, são livres no trânsito das conexões, quando não segurados por terceiros ou devidamente protegidos através de um sistema de criptografia. Dessa afirmação, gera-se um sentimento de insegurança na Internet decorrente da vulnerabilidade técnica que, possivelmente, poderá atingir o usuário. Isso porque, para a promoção de uma conexão segura, ainda é necessário um conhecimento no mínimo intermediário sobre sistemas computacionais. Por essa razão, o consumidor desprotegido poderá ter a privacidade dos seus dados corrompida por sistemas não autorizados na Internet.

Os dispositivos legais mencionados acima possuem clara conexão com a Internet das Coisas e o novo mundo de dados explorado no capítulo anterior. Assim, desde a elaboração do design na produção dos dispositivos[401], até o

[400] MADALENA, Juliano. Comentários ao Marco Civil da Internet - Lei 12.965, de 23 de abril de 2014. *Revista de Direito do Consumidor*, v. 94, p. 332, jul./ago. 2014.

[401] ZANATTA, Rafael A. F. Internet das Coisas: privacidade e segurança na perspectiva dos consumidores [Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017] – Instituto Brasileiro de Defesa do Consumidor, 2017, p. 4: "Conforme notado por estudos técnicos da área e pela própria consulta pública, os riscos são elevados, considerando que as vulnerabilidades existem no 'software utilizado pelo dispositivo, na gestão de identidade e controle de acesso e na comunicação entre dispositivos e sistemas'. O Idec reforça o entendimento firmado pela *Federal Trade Commission* de que as regras de segurança devem ser aplicadas no processo de design e *não posteriormente*. As empresas precisam (1) conduzir avaliação de risco e privacidade,

tratamento futuro das informações produzidas, é preciso que as empresas estejam atentas à criação de mecanismos que assegurem a proteção da privacidade e segurança dos usuários.

Apesar de o MCI ter representado um avanço significativo ao conseguir uma regulação ampla da Internet, bem como a garantia dos direitos básicos dos usuários, traz uma normatividade ainda insuficiente para a tutela completa do cidadão no mundo de IoT.

O MCI pode ser considerado insuficiente para uma tutela geral do cidadão no cenário de IoT em primeiro lugar (e deveras óbvio), pelo fato de que é aplicável somente aos ambientes *online*, não sendo aplicável, portanto, aos abusos à privacidade ocorridos no mundo físico. [402]

Além disso, dentre os pontos que não receberam previsão na lei e cuja ausência causará mais impactos num cenário de Internet das Coisas, destaca-se que não foi prevista a criação de um órgão público especializado (ou a atribuição de competência a um órgão já existente) com a finalidade de fiscalizar o tratamento dos dados pessoais dos usuários-consumidores[403].

Outro ponto fundamental que deve ser considerado consiste no fato de que o MCI não traz definições conceituais importantes para coibir a coleta, o tratamento abusivo e a monetização dos dados. O texto legal deixa em aberto, por exemplo, o significado das expressões "dados pessoais" e "dados sensíveis". Sem uma conceituação clara, não há como limitar de maneira efetiva os abusos dos provedores e atribuir responsabilidade jurídica por coleta excessiva ou ilegal de dados.

Por fim, o recurso do consentimento do usuário como elemento central para o uso de seus dados pessoais (refere-se à necessidade de "**consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais**")

---

(2) minimizar o conjunto de dados coletados e retidos (princípio da necessidade), e (3) testar as medidas de segurança antes de lançar produtos."

[402] PRADO, Eduardo. Internet das Coisas vai obrigar mudanças no Marco Civil da Internet. *Convergência Digital*, 2014. Disponível em: <http://sis-publique.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=37768&sid=15. Acesso em: 27 mar. 2017.

[403] HORN, Luiz Fernando Del Rio; LIMBERGER, Têmis. O diálogo entre o Marco Civil da Internet e o Código de PRoteção e Defesa do Consumidor: uma convivência legislativa em prol de um elevado nível de proteção aos dados. In: CONPEDI/UFPB. Direito do consumidor I [Recurso eletrônico on-line]. Coordenadores: Fernando Antônio de Vasconcelos, Viviane Coêlho de Séllos Knoerr, Fernando Rodrigues Martins. Florianópolis : *CONPEDI*, 2014, p. 147.

tem se mostrado ineficaz diante de recorrentes abusos contidos nos termos de uso dos provedores e seu descompasso com os direitos humanos. Esse assunto foi amplamente explorado em estudo realizado pela FGV em parceria com o Conselho da Europa: "*Terms of Service and Human Rights*."[404]

Ademais, ainda que esse dispositivo fosse eficazmente aplicado, no cenário de IoT onde a comunicação de dados é feita de forma acelerada e constante entre máquinas e humanos, a necessidade de ter a todo momento um consentimento expresso para a coleta, uso, armazenamento e tratamento de dados seria de toda maneira inviável na prática.

Alguns dos aspectos não tratados pelo Marco Civil foram previstos em Decreto, uma vez que que a lei 12.655 é de base principiológica, contando com uma escassez de detalhes sobre sua implementação.[405] O Decreto nº 8771/2016 regulamenta o Marco Civil da Internet e trata, dentre outras coisas, sobre procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações. O art. 13[406] trata dos padrões de segurança que devem ser observados por tais provedores.

[404] MAGRANI, Eduardo et. al. *Terms of Service and Human Rights*: an analysis of online platform contracts. Rio de Janeiro: Revan, 2016, p. 74.

[405] LEMOS, Ronaldo e AFFONSO, Carlos. *Marco Civil da Internet Construção e Aplicação*. p. 30.

[406] Decreto nº 8771/2016, Art. 13. "Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e
IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.
§ 1º Cabe ao CGIbr promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificidades e o porte dos provedores de conexão e de aplicação.
§ 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:
I - tão logo atingida a finalidade de seu uso; ou
II - se encerrado o prazo determinado por obrigação legal.

Complementarmente, o Instituto de Defesa do Consumidor ("Idec")[407] destaca três principais eixos que devem receber atenção a fim de assegurar a proteção dos consumidores no quesito segurança. São eles: (i) *confidencialidade dos dados e proteção à privacidade*, o que deve ser feito por meio da observância de normas já existentes, como o Marco Civil, que tratem sobre o tema da aprovação de uma lei geral de proteção de dados pessoais e da garantia de *enforcement* aos artigos 11 e 12 do referido diploma[408], para que não se crie um "regime regulatório frouxo"; (ii) *atualizações e vulnerabilidade*[409], sendo necessário pensar em formas de obrigar os fornecedores a promoverem atualizações de sistema, correções de vulnerabilidade dos produtos e garantia de

[407] ZANATTA, Rafael A. F. Internet das Coisas: privacidade e segurança na perspectiva dos consumidores [Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017] – Instituto Brasileiro de Defesa do Consumidor, 2017.

[408] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de Internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o *caput* sua filial, sucursal, escritório ou estabelecimento situado no País.

[409] Sobre o tema, Cf. MCAFEE LABS. Previsões sobre ameaças em 2017. nov. 2016, p. 23. Disponível em: <https://www.mcafee.com/br/resources/reports/rp-threats-predictions-2017.pdf>. Acesso em: 24 fev. 2017: Durante os próximos dois a quatro anos, veremos mais casos de dispositivos IoT utilizados como portas para roubo de dados e de propriedade intelectual, interrupção de infraestruturas críticas e outros grandes ataques. Muitos dispositivos IoT novos que estão entrando no mercado têm pouca ou nenhuma segurança. Os dispositivos IoT já em uso frequentemente têm pontos fracos semelhantes ou vulnerabilidades conhecidas que não podem ser corrigidas ou atualizadas. Em outros casos, dispositivos inócuos são conectados à rede sem isolamento ou segmentação apropriada, inadvertidamente proporcionando acesso a ambientes confiáveis. Finalmente, existe uma pressão operacional: 'Se está funcionando, não mexa!' Esses elementos se somam a dispositivos IoT tornando-se janelas abertas para muitos tipos de sistemas e organizações."

proteção dos dados, além da manutenção da regra de "responsabilidade solidária por lesão causada ao consumidor na cadeia de tratamento de dados pessoais"; e (iii) *dispositivos, ataques e franquias*, pois há a preocupação de que dispositivos sejam utilizados como instrumentos para spams ou ataques do tipo *denial of service* (**DDoS**, do inglês Distributed Denial-of-Service attack), além da preocupação que há no Brasil quanto ao consumo mensal de dados trafegados, o que pode trazer sérias consequências para o uso da Internet das Coisas.

Por exemplo, caso haja limitação de navegação na Internet (planos de Internet por franquia, por exemplo), um dispositivo de *IoT* pode vir a ser invadido com o intuito de aumentar o tráfego de dados (ataques do tipo DDoS) para esgotar a franquia contratada pelo consumidor, fazendo com que ele tenha que adquirir uma nova franquia.

Apesar de ser uma lei recente e atenta ao potencial que a Internet possui no nosso sistema democrático, capaz de tutelar minimamente a privacidade e os dados pessoais nos ambientes online, o MCI não é capaz de representar uma tutela suficiente e eficaz ao novo mundo de dados que se abre com a IoT, considerando tanto seu potencial quanto seus riscos a direitos fundamentais.

Exemplo de importante situação não contemplada expressamente pelo MCI é o serviço de *clouds*, amplamente utilizado atualmente. As nuvens são espaços regidos por uma rede global de servidores, que atuam fornecendo conteúdo ou serviços[410], nos quais os usuários podem armazenar qualquer tipo de arquivo, como por exemplo textos, fotos e vídeos, e acessá-los de qualquer dispositivo conectado à internet, a qualquer momento.

Ocorre que os dispositivos de IoT, por serem conectados, têm a capacidade de coletar diversos dados do usuário e armazená-los não somente em uma memória local própria, mas na nuvem da empresa que os idealizou ou de terceiros, sem que o usuário tenha conhecimento. O grande inconveniente por trás disto é que não se sabe como os dados são armazenados e tratados, surgindo uma preocupação com a segurança da informação.

Nos casos em que o provedor e/ou servidor encontram-se no Brasil e/ou quando a prestação do serviço é voltada para cidadãos brasileiros, realizada por

[410] Disponível em: < https://azure.microsoft.com/pt-br/overview/what-is-the-cloud/ >. Acesso em: 07 fev. 2016.

empresa com sede no território nacional ou que colete/processe dados em nosso território, a responsabilização por possíveis danos é prevista nos dispositivos do MCI, bem como no Código de Defesa do Consumidor.

O MCI define em seu artigo 11 que em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Define, ainda, que estas disposições aplicam-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil, ainda que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

O desafio maior é quando o servidor encontra-se em outro país ou quando não há sede em território nacional, pois a legislação brasileira não é tão clara e eficaz a respeito da jurisdição. Tal lacuna prejudica o usuário não apenas como consumidor do serviço, mas enquanto detentor dos dados, sendo ainda um óbice quanto à responsabilização do provedor/servidor em caso de vazamento ou uso indevido de conteúdo disposto na nuvem.

Portanto, apesar de termos hoje tanto a segurança quanto a privacidade do usuário tuteladas em diplomas vigentes como o CDC e o MCI, é necessário e premente que tenhamos uma lei geral que proteja a privacidade e os dados pessoais dos usuários de modo mais minucioso e atento aos âmbitos *online* e *offline (*com cuidado para que tal regulação não represente um entrave ao avanço tecnológico), nos quais dispositivos de IoT poderão atuar, colhendo dados e informações pessoais relevantes. Essa medida deve ser acompanhada, ainda, da adoção de ferramentas técnicas importantes para a garantia adequada dos direitos fundamentais na Internet das Coisas, como veremos à frente.

Nesse sentido, finalmente, passaremos a explorar agora os caminhos trilhados até então, tanto pela sociedade civil, quanto pelos poderes legislativo e executivo, para uma lei geral de proteção de dados pessoais no Brasil.

2.3
Caminhos para uma Lei Geral de Proteção de Dados Pessoais no Brasil

Desde as mais remotas origens do conceito jurídico de privacidade, que para Samuel D. Warren e Louis D. Brandeis implicava, em artigo de 1890, no direito de ser deixado só (*right to be alone*)[411], já se via a necessidade de tutelar a proteção de dados pessoais. Com o desenvolvimento social e tecnológico, diferentes facetas deste princípio surgiram[412] e novos conflitos e problemas eclodiram, como o debate sobre o direito de não tomar conhecimento sobre um dado pessoal[413], a discussão sobre biografias não-autorizadas[414] e o difícil enquadramento da privacidade no atual mundo de dados[415] refletido na IoT e nas esferas públicas conectadas.[416]

O direito à privacidade, esfera do direito à vida privada, está intimamente conectado à proteção da dignidade e personalidade humanas[417], e pode ser

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

[412] Caitlin Mulholland, por exemplo, apresenta três concepções sobre o direito à privacidade, quais sejam, "(i) o direito de ser deixado só, (ii) o direito de ter controle sobre a circulação dos dados pessoais, e (iii) o direito à liberdade das escolhas pessoais de caráter existencial" e acrescenta a esta lista o direito de não tomar conhecimento acerca de um dado pessoal". (MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. *Civilistica.com*, Rio de Janeiro, v. 1, n. 1, p. 3, 2012).

[413] Mulholland apresenta caso no qual um paciente fizera exame para pesquisar, dentre outros, a existência do vírus da Hepatite C e recebeu, em virtude de o exame de sangue conduzido pelo laboratório ter sido outro que não o solicitado, o resultado positivo do exame anti-HIV. Para Mulholland, "divulgação à pessoa de dado não requisitado configura violação ao seu direito de não saber e gera, incontestavelmente, o direito à indenização por danos morais". Confira-se: MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. *Civilistica.com*, Rio de Janeiro, v. 1, n. 1, p. 1-11, 2012

[414] Sobre o tema, v. MORAES, Maria Celina Bodin de. Biografias não autorizadas: conflito entre a liberdade de expressão e a privacidade das pessoas humanas? Editorial. *Civilistica.com*, Rio de Janeiro, v. 2, n. 2, p. 1-4, 2013.

[415] Confira-se, sobre o tema, SLOAN, Robert H.; WARNER, Richard. *Unauthorized Access*: The Crisis in Online Privacy and Security. London/New York: CRC Press, 2014; MADDEN, Mary. Privacy management on social media sites. A Project of the Pew Research Center. Disponível em: <http://www.isaca.org/Groups/Professional-English/privacy-data-protection/GroupDocuments/PIP_Privacy%20mgt%20on%20social%20media%20sites%20Feb%202012.pdf>. Acesso em: 07 fev. 2016.

[416] MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.

[417] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*. São Paulo: Editora Revista dos Tribunais, 2012, p. 390.

extraído do reconhecimento constitucional dado à intimidade, à vida privada[418] e à inviolabilidade de dados[419]. Dentre as previsões constitucionais sobre o tema, destaca-se que a Constituição Federal de 1988 apontou o *habeas data* como instrumento apto a assegurar a proteção de informações e dados pessoais[420]-[421].

Conforme visto nos itens anteriores deste capítulo, a privacidade também recebeu proteção infraconstitucional no Brasil. O Código Civil protege diretamente a vida privada[422] e também o Código de Defesa do Consumidor o faz, dedicando a Seção VI à proteção de bancos de dados e de cadastros dos consumidores. Complementarmente, o Marco Civil da Internet, vigente desde 2014, trouxe dispositivos destinados à proteção da privacidade, que constitui um dos pilares da Lei. O inciso II do artigo 3º elenca tal proteção como princípio a ser observado na disciplina da Internet, como o é a proteção de dados, prevista no inciso III. Destacamos, ainda, os artigos 7º e 10, que também abordam o tema. Nada obstante, a regulação do Marco Civil é insuficiente para proteger os dados pessoais e a privacidade em suas mais diversas facetas. Não há, no ordenamento brasileiro, uma lei específica de proteção a dados pessoais. Entretanto, há importantes projetos de lei em tramitação.

Na nova sociedade da informação, a privacidade deve ser entendida de forma funcional, de modo a assegurar a um sujeito a possibilidade de "conhecer,

[418] Constituição Federal de 1988, art. 5º (...) 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;

[419] Constituição Federal de 1988, art. 5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

[420] Constituição Federal de 1988, art. 5º, LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

[421] A doutrina destaca que apesar de haver alguns instrumentos no ordenamento jurídico brasileiro e até leis que se destinam a proteger a privacidade, é preciso de algo mais específico: "Although some problems regarding data protection in Brazil require enforcement measures (…), there are some issues that can only be adequately addressed by a broad regulation such as a comprehensive data protection act. This would increase the legal certainty of business activities against the risks to privacy arising from data processing. This explains why there have been many attempts to create a general legal framework for data protection in Brazil." (DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul De. (Eds.) *Reloading Data Protection*: Multidisciplinary Insights and Contemporary Challenges. London: Springer, 2014, p. 15).

[422] Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

controlar, endereçar, interromper o fluxo das informações a ele relacionadas"[423]. Neste exato sentido, Stefano Rodotá complementa, definindo sinteticamente a proteção da privacidade como "o direito de manter o controle sobre as próprias informações"[424].

Nesta concepção, a privacidade não tem apenas o caráter de liberdade negativa – isto é, a liberdade de não ser impedido ou de não ser obrigado a fazer algo[425] –, mas também o de liberdade positiva – ou seja, liberdade como autonomia, liberdade enquanto possibilidade de direcionar seu próprio querer sem ser determinados por outros[426-427] –, ligada ao controle dos dados. Essa perspetiva deriva do contexto social advindo de evoluções tecnológicas no qual a informação assume um papel de bem econômico e "elemento estruturante para o desenvolvimento das relações sociais, sendo, pois, o signo maior desta anunciada e consolidada revolução socioeconômica"[428].

O fator tecnológico possui papel de destaque uma vez que, com a melhora da capacidade de armazenamento e de comunicação de informações, surgem novas maneiras de organizar, utilizar e apropriar a informação[429]. Como destaca Danilo Doneda, "esta crescente importância traduz-se no fato de que uma

[423] RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 92.

[424] Ibid.

[425] Como conceitua Norberto Bobbio, "[p]or liberdade negativa, na linguagem política, entende-se a situação na qual um sujeito tem a possibilidade de agir sem ser impedido, ou de não agir sem ser obrigado, por outros sujeitos. (...) A liberdade negativa costuma também ser chamada de liberdade como ausência de impedimento ou de constrangimento: se, por impedir, entende-se não permitir que outros façam algo, e se, por constranger, entende-se que outros sejam obrigados a fazer algo, então ambas as expressões são parciais, já que a situação de liberdade chamada de liberdade negativa compreende tanto a ausência de impedimento, ou seja, a possibilidade de fazer, quanto a ausência de constrangimento, ou seja, a possibilidade de não fazer." (BOBBIO, Norberto. *Igualdade e liberdade*. Tradução: Carlos Nelson Coutinho. 2. ed. Rio de Janeiro: Ediouro, 1997, p. 48-49).

[426] Para Bobbio, [p]or liberdade positiva, entende-se -na linguagem política -a situação na qual um sujeito tem a possibilidade de orientar seu próprio querer no sentido de uma finalidade, de tomar decisões, sem ser determinado pelo querer de outros. Essa forma de liberdade é também chamada de autodeterminação ou, ainda mais propriamente, de autonomia" (BOBBIO, Norberto. *Igualdade e liberdade*. Tradução: Carlos Nelson Coutinho. 2. ed. Rio de Janeiro: Ediouro, 1997, p. 51).

[427] Sobre o tratamento da privacidade como liberdade negativa ou positiva, v. MACEDO JÚNIOR, Ronaldo Porto. Privacidade, Mercado e Informação. *Justitia*, São Paulo, n. 61, p. 245-259, jan./dez. 1999.

[428] BIONI, Bruno Ricardo. A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. In: ROVER, Aires José; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo. *Direito e novas tecnologias*. Florianópolis: CONPEDI, 2014, p. 65.

[429] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 153.

considerável parcela das liberdades individuais hoje são concretamente exercidas através de estruturas nas quais a comunicação e a informação têm papel relevante"[430].

O desenvolvimento tecnológico permite a criação de perfis de comportamento que podem até se confundir com a própria pessoa[431]. Tais perfis, aliados à manipulação de dados colhidos, pode gerar sérios impactos na liberdade dos indivíduos. Conforme nos explica Doneda sobre a técnica de coleta de dados pessoais conhecida como *data mining*: [432]

> Ela consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos. Assim, a partir de uma grande quantidade de informações em estado bruto e não classificada, podem ser identificadas informações de potencial interesse.

Portanto, se por um lado a tecnologia traz inegáveis benefícios à sociedade como um todo, cria, de outro lado, problemas à proteção da privacidade. Para Stefano Rodotá, apesar de a tecnologia ajudar a moldar uma esfera privada mais rica, contribui para que essa esfera seja cada vez mais frágil e exposta a ameaças, "daí deriva a necessidade do fortalecimento contínuo de sua proteção jurídica e da ampliação das fronteiras do direito à privacidade"[433].[434] As mudanças sociais e tecnológicas exigem uma proteção específica da privacidade e, em particular, dos dados pessoais. Nas palavras de Carlos Affonso Pereira: [435]

---

[430] Ibid, p. 153-154.

[431] Como pontua Danilo Doneda, na técnica *profiling*, "os dados pessoais são tratados, com o auxílio de métodos estatísticos, técnicas de inteligência artificial e outras mais, com o fim de obter uma 'metainformação', que consistira numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destinos de uma pessoa ou grupo." (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 173).

[432] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 176.

[433] RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 95.

[434] Cabe destacar que o ordenamento jurídico brasileiro já prevê, no texto constitucional, a proteção da privacidade e da inviolabilidade de dados, além de apontar o *habeas data* como instrumento apto a assegurar a proteção deste direito. Porém, as mudanças sociais e tecnológicas exigem uma proteção mais ampla da privacidade.

[435] SOUZA, Carlos Affonso Pereira de. O progresso tecnológico e a tutela jurídica da privacidade, *Direito, Estado e Sociedade*, n. 16, p. 8, jan./jul. 2000. Em sentido similar, Bruno Bioni afirma: "Defende-se, assim, uma guinda da *produção normativa* para que não se tutela a privacidade negativamente, mas, positivamente, premiando, sobretudo, práticas que assegurem o tão desejado controle de informações por parte dos usuários da *Internet*." (BIONI, Bruno Ricardo. A produção

> O alcance das mudanças que nascem no meio social a partir da difusão de tais tecnologias impõe, por seu turno, o aperfeiçoamento da regulamentação jurídica então existente visando estabelecer soluções para os conflitos que venham a surgir. Vale destacar que nem sempre a edição de novas regras se faz necessária frente ao avanço tecnológico, todavia ordinariamente a sofisticação no manuseio de técnicas em constante evolução requer a tutela legal de suas peculiaridades.
> (...)
> A proteção do direito à privacidade perante o progresso tecnológico e a faculdade de acesso e distribuição indevida de dados de terceiros tornou-se um desses conflitos, demandando o trabalho não apenas dos juristas, mas igualmente dos legisladores e magistrados no sentido de se definir o *locus* da privacidade no cenário contemporâneo.
> (...)
> A concepção do direito à privacidade como proteção do isolamento individual encontra-se aquém da tutela requerida pela intensa movimentação de dados pessoais na Internet. Assim, o controle da coleta, armazenamento e utilização de dados torna-se imperativo, sendo essa a função primordial que tem a desempenhar o direito à privacidade frente às novas tecnologias.

Como Danilo Doneda e Laura Mendes pontuam, a proteção de dados tem sido alvo de crescente atenção no Brasil, mas há a necessidade de se criar instrumentos legais para lidar com as novas tecnologias: [436]

> Pode-se observar que a proteção de dados está se tornando um campo autônomo no Brasil e ganhando relevância dentro do sistema legal. Portanto, é de se esperar que os últimos desenvolvimentos em tecnologia da informação demandem cada vez mais a criação de novos instrumentos de proteção de dados no Brasil para lidar com os riscos à privacidade individual apresentados, por exemplo, pelo onipresente processamento de dados, Internet das Coisas, pesquisas online e pela web 2.0. A atual revisão da Diretiva Europeia e do Livro Branco sobre a privacidade digital, publicado pelo governo dos EUA, ambos do ano de 2012, indicam a necessidade de se criarem novos instrumentos jurídicos relativos à privacidade e à proteção de dados para lidar com o progresso tecnológico e a globalização. Não há dúvida de que o sistema brasileiro de proteção de dados deve continuar a se desenvolver, a fim de garantir os direitos fundamentais e a segurança jurídica em uma sociedade conectada. [437]

---

normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. In: ROVER, Aires José; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo. *Direito e novas tecnologias*. Florianópolis: CONPEDI, 2014, p. 80).

[436] DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul De. (Eds.) *Reloading Data Protection*: Multidisciplinary Insights and Contemporary Challenges. London: Springer, 2014, p. 19.

[437] Tradução livre do autor. No original: *It can be observed that data protection is becoming an autonomous field in Brazil and gaining relevance within the legal system. It is therefore to be expected that the latest developments in information technology will increasingly demand the creation of new data protection instruments in Brazil to deal with the risks to individual privacy presented, for example, by the ubiquitous data processing, the Internet of things, online searching and the web 2.0. The current revision of the European Directive and the white paper on digital privacy, released by the U.S. government, both in the year 2012, indicate the need to create new legal instruments concerning privacy and data protection to deal with technological progress and*

O governo brasileiro, diante do cenário nacional e internacional de intensas inovações tecnológicas e das consequências sobre o direito à privacidade, passou a reconhecer, de forma paulatina, que a garantia de direitos fundamentais em face das novas tecnologias demanda a edição de marcos legais.

Assim, teve início a elaboração, em 2010, de forma colaborativa entre o Ministério da Justiça e a sociedade, da primeira versão do que viria a ser um dos Projetos de Lei sobre a proteção de dados pessoais em tramitação no Congresso Nacional. O objetivo precípuo de tal medida desde aquela época até hoje é, dentre outras coisas, a garantia da liberdade, privacidade e intimidade das pessoas.[438]

O impulsionamento para uma maior proteção da privacidade, sobretudo no cenário online, adveio de acontecimentos relativos a vazamentos de informações e à edição de leis gerais para proteção de dados em países estrangeiros. Dentre os vazamentos, destaca-se as revelações feitas por Edward Snowden acerca da espionagem do governo americano em nível mundial, que atingiu chefes de estado, como os do Brasil (Dilma Roussef, à época) e da Alemanha (Angela Merkel)[439], os quais apresentaram à Assembleia Geral da ONU uma proposta com regras para proteger o direito à privacidade na era digital[440].

No que tange a normas estrangeiras, diversos países da América Latina já possuem leis de proteção a dados pessoais. Neste sentido, há leis promulgadas, por exemplo, na Argentina, no Chile e na Colômbia[441]. Já na Europa, todos os países, com exceção da Bielorrússia, possuem leis de proteção de dados

---

globalization. There is no doubt that the Brazilian data protection system must continue to develop, in order to guarantee fundamental rights and legal certainty in a networker society.

[438] https://economia.uol.com.br/ultimas-noticias/infomoney/2011/06/15/ministerio-da-justica-quer-lei-sobre-privacidade-e-protecao-de-dados-pessoais.jhtm.

[439] Sobre o tema, v. BIONI, Bruno Ricardo. A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. In: ROVER, Aires José; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo. *Direito e novas tecnologias*. Florianópolis: CONPEDI, 2014, p. 62-85; LUCAS JR., George R. NSA Management Directive #424: Secrecy and Privacy in the Aftermath of Edward Snowden. *Ethics & International Affairs*, v. 28, n. 1, p. 29-38, 2014.

[440] MATOSO, Filipe. Dilma diz que privacidade na Internet deve ter tratamento prioritário na ONU. *G1*, Brasília, 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/11/dilma-diz-que-privacidade-na-Internet-deve-ter-tratamento-prioritario-na-onu.html>. Acesso em: 07 fev. 2017.

[441] BANISAR, David. National Comprehensive Data Protection/Privacy Laws and Bills 2016. *ARTICLE 19: Global Campaign for Free Expression*, 2016. Disponível em: <https://ssrn.com/abstract=1951416>. Acesso em: 07 fev. 2017.

pessoais [442]. Neste continente, com os vazamentos sobre os programas de vigilância dos Estados Unidos, os eurodeputados agiram de modo a fortalecer as regras já existentes desde 1995. Assim, votaram a reforma das regras europeias acerca da proteção de dados pessoais, buscando assegurar aos usuários da Internet maior controle sobre seus dados e sujeitar transferências de dados pessoais processados na União Europeia para fora desta a requisitos mais severos[443].

No Brasil, o esboço do primeiro PL foi levado a debate público através do blog[444] criado pelo Ministério da Justiça (MJ) em conjunto com o Observatório Brasileiro de Políticas Digitais do Comitê Gestor da Internet no Brasil (CGI). Desta forma, os usuários puderam, através de comentários aos posts, deliberar sobre as proposições do futuro PL, bem como sugerir alterações ao texto. Com o fim da consulta, em 2011, o MJ consolidou as propostas num texto final, que deu origem ao PL nº 4060/2012[445].

Durante os anos que se seguiram, diversos congressos e seminários[446] foram realizados com o fim de amadurecer as discussões e permitir a elaboração de propostas eficazes para a proteção dos dados e consecução dos direitos fundamentais envolvidos.

Entre os anos 2013 e 2014, foram propostos os PLs n° 330/2013[447], nº 181/2014[448] e nº 131/2014[449], que dispunham sobre a proteção de dados pessoais em geral e o fornecimento de dados de cidadãos e/ou empresas brasileiras a organismos estrangeiros, frutos da CPI da Espionagem levada a cabo pelo Senado

---

[442] Ibid.

[443] Disponível em: <http://www.europarl.europa.eu/news/pt/news-room/20140307IPR38204/parlamento-europeu-refor%C3%A7a-prote%C3%A7%C3%A3o-dos-dados-pessoais-dos-cidad%C3%A3os>. Acesso em: 27 mar. 2017.

[444] Disponível em: <http://pensando.mj.gov.br/dadospessoais2011/>. Acesso em: 28 fev. 2017.

[445] Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066&ord=1>. Acesso em: 27 mar. 2017.

[446] Como exemplo temos: o Seminário sobre Privacidade e Proteção de Dados Pessoais organizado pela CGI (http://seminarioprivacidade.cgi.br/#about); o Seminário Direito Digital e a (des)proteção de Dados (http://www.insper.edu.br/educacao-executiva/cursos-de-curta-duracao/seminario-direito-digital-e-a-des-protecao-de-dados-integral/) organizado pela Insper; e o Seminário Compliance em Privacidade e Proteção de Dados Pessoais organizado pela TI Rio (http://www.tirio.org.br/info/36363/20-seminario-compliance-em-privacidade-e-protecao-de-dados-pessoais)

[447] Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 27 mar. 2017.

[448] Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/117736>. Acesso em: 27 mar. 2017.

[449] Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/116969>. Acesso em: 27 mar. 2017.

Federal[450]. Em 2015, estes três projetos foram apensados e tramitam em conjunto até hoje.

No início de 2015, o Ministério da Justiça realizou outro debate público para discutir a nova minuta do anteprojeto de proteção de dados pessoais. Desta vez as discussões ocorreram por meio de uma plataforma desenvolvida pelo próprio MJ, como parte do Projeto Pensando o Direito[451]. Para deliberar, os usuários deveriam se cadastrar, selecionar o debate específico sobre Proteção de Dados Pessoais e depois comentar o trecho da lei que desejassem; havia também a possibilidade de "curtir" os outros comentários que eram colocados ou, ainda, de debater genericamente os eixos que orientam o anteprojeto[452], além de dar sugestões sem se ater ao texto preexistente. O debate foi frutífero e contou com relevante participação dos cidadãos, tendo sido contabilizados 1800 comentários. O processo ficou muito mais claro e eficiente, contando ainda com a utilização das redes sociais, na medida em que foram criados Twitter, Facebook e YouTube próprios para o debate[453].

A página "Pensando o Direito" colocou à disposição dos usuários, inclusive, um panorama da proteção de dados pessoais ao redor do mundo e como foi ou tem sido o processo de elaboração de uma lei sobre o assunto[454]. Isto facilitou a realização de uma análise comparativa da experiência internacional pela própria sociedade civil para que, assim, se tivesse uma maior ideia de quais disposições poderiam ser transplantadas para o Brasil.

---

[450] Disponível em: <http://www12.senado.leg.br/noticias/materias/2015/10/13/marco-regulatorio-para-protecao-de-dados-pessoais-e-aprovado-pela-cct-e-segue-para-tres-outras-comissoes>. Acesso em: 27 mar. 2017.

[451] O Projeto Pensando o Direito foi criado pelo Ministério da Justiça como uma forma de tornar o processo de elaboração legislativa mais próximo da sociedade, tornando-o, assim, mais democrático. Uma das formas encontradas para fazê-lo foi exatamente a realização de consultas públicas online durante determinado período de tempo, antes do envio do projeto de lei ao Congresso Nacional. A plataforma do debate em questão é similar à utilizada na deliberação acerca do Marco Civil da Internet, de Crimes Contra a Corrupção, dentre outros.

[452] São eles: escopo e aplicação; dados pessoais, dados anônimos e dados sensíveis; princípios; consentimento; término do tratamento; direitos do titular; comunicação, interconexão e uso compartilhado de dados; transferência internacional de dados; responsabilidade dos agentes; segurança e sigilo de dados pessoais; boas práticas; como assegurar estes direitos, garantias e deveres?; e disposições transitórias.

[453] Twitter: @dadospessoais; Facebook: https://www.facebook.com/Debate-P%C3%BAblico-Prote%C3%A7%C3%A3o-de-Dados-Pessoais-170882592934972/; Youtube: Disponível em: <https://www.youtube.com/channel/UC4xogFvkir1ypVRKZeUsg5A>. Acesso em: 27 mar. 2017.

[454] Disponível em: <http://pensando.mj.gov.br/dadospessoais/2015/04/protecao-de-dados-pessoais-pelo-mundo/>. Acesso em: 15 mar. 2017.

Ainda em 2015 foram realizadas duas audiências públicas: uma no Senado, para discutir os três PLs e outra na Câmara dos Deputados, para discutir o PL nº 4060/2012.

Como conclusão do processo de deliberação pública desencadeado pelo Ministério da Justiça em 2015, o "Anteprojeto de Lei de Proteção de Dados Pessoais" (PL nº 5276/2016) foi proposto em 2016 pelo Poder Executivo e, atualmente, tramita na Câmara dos Deputados.

É de salientar que o Anteprojeto nº 5276/2016 foi recebido com urgência pela Câmara dos Deputados e, posteriormente, foi apensado ao PL nº 4060/2012. Com esta unificação, ambos os projetos passaram a tramitar pelo rito prioritário, o que significa que as Comissões terão, em princípio, dez sessões para deliberar sobre eles. Em decisão recente (24/08/2016), o Presidente da Câmara dos Deputados determinou a criação de uma Comissão Especial encarregada de discutir o PL nº 4060/2012.

Os PLs em tramitação no Senado Federal, por sua vez, já foram aprovados pela Comissão de Tecnologia, Inovação, Comunicação e Informática e pela de Meio Ambiente, Defesa do Consumidor e Fiscalização e Controle. Desde 14/07/2016 aguardam a apresentação do relatório e subsequente votação na Comissão de Assuntos Econômicos.

Aliado ao Marco Civil da Internet e seu respectivo decreto regulamentar, à Política de Dados Abertos do Governo Federal e ao Programa Brasil Inteligente, a deliberação acerca da lei de proteção de dados pessoais representa grande avanço nas questões de políticas digitais, inserindo esta pauta no cenário político brasileiro. Uma linha do tempo detalhada sobre o assunto pode ser consultada no site: http://dataprivacy.com.br/. Sendo assim, os vários anos de deliberação acerca da viabilidade de uma lei brasileira de Proteção de Dados Pessoais foram importantes para o amadurecimento dos projetos e são mais um exemplo de processo legislativo participativo, que contou com mais de 1800 comentários.

A necessidade de uma lei geral que assegure a proteção de dados pessoais se aprofunda no cenário da Internet das Coisas (*Internet of Things – IoT*)[455]. Como

[455] "Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, conseqüentemente, a sua divulgação, foram facilitados de forma extrema. Como resultado, existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não

pontua Stefano Rodotá, a noção de vida privada vem sendo expandida devido, dentre outros fatores, ao desenvolvimento da tecnologia.

Assim, o conceito passa a abranger o "conjunto de ações, comportamentos, opiniões, preferências e informações pessoais sobre os quais o interessado pretende manter um controle exclusivo"[456]. A concepção do que seja privado, "tende a abranger o conjunto das atividades e situações de uma pessoa que tem um potencial de 'comunicação', verbal e não-verbal, e que pode, portanto, se traduzir em informações"[457].

No contexto de Internet das Coisas, a crescente conectividade com os mais diversos dispositivos de tecnologia gera uma fonte praticamente inesgotável de informações acerca do dia a dia dos usuários de tais dispositivos. Tendo em vista que ao se falar em privado temos em mente informações de caráter pessoal[458], é imprescindível dedicar especial proteção aos dados e às informações geradas através da IoT. Com isso, salta aos olhos a indispensabilidade de uma lei de proteção de dados pessoais que, nas palavras de Doneda, "merecem uma atenção particular, seja pela dinamicidade de seu conteúdo como pelo novo cenário que procura regular, marcado pela forte presença da tecnologia"[459]. É necessário, portanto, ajustar as leis e conceitos jurídicos sobre o tema para que as pessoas possam confiar na infraestrutura da Internet das Coisas, acreditando na proteção existente de seus dados pessoais[460].

---

autorizado de terceiros a esses dados. Com isso, a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada." (MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. *Civilistica.com*, Rio de Janeiro, v. 1, n. 1, p. 3, 2012)

[456] RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 92.

[457] Ibid, p. 93.

[458] Ibid.

[459] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 362. Em sentido similar, Carlos Affonso de Souza afirma que "as ameaças ao direito à privacidade foram severamente incrementadas na medida em que o progresso tecnológico permitiu maiores facilidades ao indivíduo. O tratamento da informação por computadores permite não apenas seu célere processamento para fins idôneos, mas também para o célere cruzamento de dados sigilosos ou a interceptação dos mesmos em uma rede, por exemplo. A Internet, expoente de tal avanço, é, por consequência, o cenário onde atualmente se discute a nova tutela demandada pela necessidade de privacidade pessoal." (SOUZA, Carlos Affonso Pereira de. O progresso tecnológico e a tutela jurídica da privacidade, *Direito, Estado e Sociedade*, n. 16, p. 23, jan./jul. 2000).

[460] ALMEIDA, Virgilio A. F.; DONEDA, Danilo; MONTEIRO, Marília. Governance Challenges for the Internet of Things. *IEEE Internet Computing*, jul./ago. 2015, p. 57: "To protect citizens'

Exploraremos a fundo no tópico seguinte as previsões regulatórias específicas contidas nas propostas de lei e seu contraste com a regulação europeia. A justificativa para essa comparação internacional se deve à forte influência da regulação europeia nos projetos de lei sobre dados pessoais no Brasil, assim como à maior compatibilidade e adequação entre o direito brasileiro e o direito europeu, razão pela qual não nos aprofundaremos neste trabalho nas especificidades da regulação norte-americana.[461]

2.4
Contrastes entre a Proposta Regulatória Brasileira e a Regulação Europeia acerca da privacidade

A proteção da privacidade é ponto fundamental de sociedades que se pretendem democráticas e está prevista como direito fundamental na Convenção Europeia de Direitos Humanos [462] e na Declaração Universal de Direitos Humanos [463]. Os tratados internacionais sobre o tema, em geral, tratam da privacidade sob o aspecto da não ingerência na vida privada familiar, da correspondência e das comunicações, assim como o faz nossa Constituição

personal data and to build people's trust in the IoT infrastructure, legal frameworks regarding data protection must be adjusted according to the nature of these new technologies".

[461] Os Estados Unidos não possuem uma única lei federal abrangente que regula a coleta e uso de informações pessoais. Os EUA regulam a privacidade e a segurança apenas em certos setores específicos (ex.: saúde e financeiro) bem como tipos de informações sensíveis, criando por vezes proteções sobrepostas e contraditórias. Portanto, por não ter uma lei abrangente proteção legal para dados pessoais, possuindo apenas algumas leis específicas setoriais, os EUA não conseguem proteger adequadamente os dados dos indivíduos. Portanto, entendemos que o sistema regulatório norte-americano está aquém de uma proteção adequada, que estaria mais próxima do modelo regulatório europeu pautado por uma compreensiva lei geral de proteção. Disponível em: <https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html>. Acesso em: 27 mar. 2017.

[462] ARTIGO 8° Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

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

Federal de 1988. A interpretação da privacidade, contudo, vem mudando substancialmente nos últimos anos e esse direito ganhando novos contornos[464].

A tecnologia faz com que a esfera privada seja moldada de forma mais rica, contudo mais frágil e exposta a ameaças.[465]. Por isso, tem-se a "necessidade do fortalecimento contínuo de sua proteção jurídica, da ampliação das fronteiras do direito à privacidade"[466]. No atual cenário, as mudanças sociais e tecnológicas exigem uma proteção específica da privacidade no Brasil e, em particular, dos dados pessoais[467].

O direito à privacidade configura um valor complexo[468], com diferentes significados e diversos aspectos que o caracterizam.[469]. Como pontua Ingo Sarlet com base em Vital Moreira e em Canotilho, o direito à privacidade envolve o direito de impedir que estranhos tenham acesso a informações sobre a vida privada e que tais informações não sejam divulgadas[470].

Há, ainda, quem trate do direito à privacidade sob a ótica do resguardo contra interferências alheias - o que implica o direito que o indivíduo possui de ser deixado em paz a fim de viver sua vida com um grau mínimo de intromissão -,

[464] Como afirma Stefano Rodotà, "As novas dimensões da coleta e do tratamento de informações provocaram a multiplicação de apelos à privacidade e, ao mesmo tempo, aumentaram a consciência da impossibilidade de confinar as novas questões que surgem dentro do quadro institucional tradicionalmente identificado por este conceito". RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 23.

[465] Na Sociedade de Informação em que vivemos atualmente, a privacidade pode ser definida, nas palavras de Stefano Rodotà como: "o direito de manter o controle sobre as próprias informações". RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 92.

[466] RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 95.

[467] DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul De. (Eds.) *Reloading Data Protection*: Multidisciplinary Insights and Contemporary Challenges. London: Springer, 2014, p. 19; BIONI, Bruno Ricardo. A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. In: ROVER, Aires José; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo. *Direito e novas tecnologias*. Florianópolis: CONPEDI, 2014, p. 80.

[468] POST, Robert C. Three Concepts of Privacy. *Georgetown Law Review*, v. 89, p. 2087, 2001.

[469] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*. São Paulo: Editora Revista dos Tribunais, 2012, p. 393-394.

[470] Ibid, p. 394.

sob a ótica do segredo ou sigilo de determinadas informações e, por fim, sob a ótica do controle sobre informações e dados pessoais[471].

O direito à privacidade não possui um conceito unívoco, mas uma ideia plural que abarca suas inúmeras facetas. Este é o cenário exposto por Danilo Doneda, que pontua que a privacidade, hoje, está relacionada à proteção dos dados pessoais: [472]

> As demandas que moldam o perfil da privacidade hoje são de outra ordem [diferentes da tutela da privacidade como o direito de ser deixado só], relacionadas à informação e condicionadas pela tecnologia. Hoje, a exposição indesejada de uma pessoa aos olhos alheios se dá com maior frequência através da divulgação de seus dados pessoais do que pela intrusão em sua habitação, pela divulgação de notícias a seu respeito na imprensa, pela violação de sua correspondência - enfim, por meios 'clássicos' de violação da privacidade.
> Ao mesmo tempo, somos cada vez mais identificados a partir dos nossos dados pessoais, fornecidos por nós mesmos aos entes, públicos e privados, com os quais mantemos relações; ou então coletados por meios diversos. Tais dados pessoais são indicativos de aspectos de nossa personalidade, portanto merecem proteção do direito enquanto tais.[473]

Como vimos, ainda não há uma lei específica destinada à proteção da privacidade na Internet. Há, porém, projetos de lei em tramitação, alguns dos quais buscaram inspiração na legislação europeia, justificando, portanto, a comparação que faremos neste trabalho.

A legislação europeia, por sua vez, foi renovada recentemente e traz uma normatividade mais completa e mais aprofundada do que as leis brasileiras existentes e os projetos de lei do país. Avaliaremos, a partir de agora, os contrastes existentes entre a regulação europeia e as propostas de regulação no Brasil acerca da privacidade.

Conforme descrito no item anterior, entre os anos 2013 e 2014, foram propostos os PLs n° 330/2013[474], nº 181/2014[475] e nº 131/2014[476], que dispunham sobre a proteção de dados pessoais em geral e o fornecimento de dados de

---

[471] Sobre os diferentes conceitos de privacidade, v. LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2011, p. 52 e ss.
[472] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 14.
[473] Ibid., p. 1.
[474] Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 27 mar. 2017.
[475] Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/117736>. Acesso em: 27 mar. 2017.
[476] Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/116969>. Acesso em: 27 mar. 2017.

cidadãos e/ou empresas brasileiras a organismos estrangeiros, frutos da CPI da Espionagem levada a cabo pelo Senado Federal[477]. Em 2015, estes três projetos foram apensados e tramitam em conjunto até hoje. Também tramitam em conjunto o PL nº 4060/2012 e o Projeto nº 5276/2016.

O Projeto nº 5276/2016, em especial, traz importantes princípios para que a proteção da privacidade e dos dados pessoais seja efetiva, prevendo, por exemplo, o princípio da finalidade[478], o princípio da adequação[479] e o princípio da necessidade[480]. Este PL sofreu forte influência da regulação europeia, guardando inúmeras semelhanças com o Regulamento Geral de Protecção de Dados (GDPR) - Regulamento (UE) 2016/679. [481] Em virtude de ser o PL mais protetivo e consistente, exploraremos melhor os contrastes entre a GDPR e o nº 5276/2016.[482]

A *General Data Protection Regulation* ("GDPR") é um regulamento pelo qual o Parlamento Europeu, o Conselho da União Europeia e a Comissão Europeia tencionam reforçar e unificar a protecção de dados para todos os

[477] Disponível em: <http://www12.senado.leg.br/noticias/materias/2015/10/13/marco-regulatorio-para-protecao-de-dados-pessoais-e-aprovado-pela-cct-e-segue-para-tres-outras-comissoes>. Acesso em: 27 mar. 2017.

[478] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades;

[479] Art.ç 6º (...) II - adequação: pelo qual o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;

[480] Art. 6º (...) III - necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

[481] Disponível em: <http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf>. Acesso em: 27 mar. 2017.

[482] Recentemente o PLs n° 330/2013 ganhou potência renovada e apoio do Poder Executivo Federal após receber um Substitutivo apresentado pelo Senador Aloysio Nunes Ferreira. O Governo tem interesse nesse momento na aprovação de uma lei geral de privacidade e proteção de dados pessoais por ambicionar inserir o Brasil no grupo de países da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) e a ausência de uma lei geral de privacidade pode ser um impeditivo.

O PLs n° 330/2013 e o Projeto de Lei n° 5.276/2016 podem ser consideradas as principais iniciativas legislativas que objetivam regulamentar de forma abrangente a proteção de dados pessoais no Brasil. O Substitutivo ao PLs n° 330/2013, no entanto, ao incluir algumas mudanças em relação ao PL n° 5.276/2016, trata determinados temas de maneira inadequada ou incompleta quando comparado ao PL n° 5.276/2016. Ambos os PLs estabelecem uma série de princípios que também figuram no GDPR, como por exemplo, a necessidade de se obter o consentimento, manifestamente livre do titular para o tratamento de seus dados. No entanto, o PL n° 5.276/2016 e o GDPR são mais precisos em suas definições e conceitos, quando comparados ao Substitutivo.

indivíduos da União Europeia (EU). Quando o GDPR entrar em vigor, ele substituirá a diretiva de proteção de dados (Diretiva 95/46 / CE) de 1995.[483]

A legislação destina-se a "harmonizar" as leis de privacidade de dados em toda a Europa, bem como a dar maior proteção e direitos aos cidadãos europeus residentes no território[484]. Após mais de quatro anos de discussão e negociação, o GDPR foi aprovado tanto pelo Parlamento Europeu como pelo Conselho Europeu em abril de 2016. Logo após, a publicação do GDPR ocorreu no Jornal Oficial da UE em maio de 2016, com previsão de entrada em vigor em 25 de maio de 2018. O período de preparação de dois anos se deu em função das empresas e órgãos públicos abrangidos pelo regulamento, de modo que estes possam se preparar para as mudanças.

O Regulamento será executável a partir de 25 de maio de 2018 e, ao contrário de uma directiva, não exige que os governos nacionais aprovem qualquer legislação interna. Portanto, é diretamente vinculativo e aplicável.

Dentro do GDPR, há grandes mudanças para o público, bem como empresas e órgãos que manipulam informações pessoais dentro e fora da UE, o que explicaremos com mais detalhes adiante.[485]

Uma das similaridades que mais chama a atenção entre o PL nº 5276/2016 e a GDPR é quanto aos princípios. O PL nº 5276/2016 tem seus princípios dispostos no art. 6º, enquanto a GDPR os prevê em seu artigo 5º. Apesar de adotarem nomenclaturas distintas, os princípios são praticamente idênticos. Segue abaixo imagem ilustrativa dos princípios garantidos pela GDPR. São eles: *lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality;*e *accountability:* [486]

---

[483] Disponível em: <http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf>. Acesso em: 27 mar. 2017.

[484] *"1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."*

[485] Disponível em: <http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>. Acesso em: 27 mar. 2017.

[486] *"Article 5 of the GDPR requires that personal data shall be:*
"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

Abaixo, tabela comparativa traçando algumas correspondências entre os princípios do GDPR e do PL 5276.

PROJETO DE LEI 5.276/16	REGULAMENTO 679 UE (GDPR)
Princípio da transparência	**Princípio da licitude, lealdade e transparência** (*lawfulness, fairness and transparency)*
Princípio da finalidade e princípio da adequação	**Princípio da limitação da finalidade** (*purpose limitation)*
Princípio da necessidade	**Princípio da minimização** (*data minimisation)*
Princípio da qualidade dos dados	**Princípio da exatidão** (*accuracy)*

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."
Article 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."." Disponível em: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/>. Acesso em: 27 fev. 2017.

Princípio da segurança	Princípio da integridade e confidencialidade (*integrity and confidentiality)*

Os princípios garantidos pelo Regulamento Geral de Proteção de Dados (GDPR), serão diretamente aplicáveis, a partir de maio de 2018, independentemente de internalização dos princípios pelos Estados-membro através da lei nacional. Estes exigem que cada controlador demonstre a conformidade com os princípios de proteção de dados.[487]

> Esta legislação vem introduzir uma mudança de paradigma na forma como todos os intervenientes olham para a proteção de dados pessoais – dos próprios cidadãos às empresas que processam os dados, passando pelos profissionais do direito". (...) O novo regulamento é aplicado em todos os estados-membros, num total de mais de 500 milhões de cidadãos, e obrigará a um importante esforço de adaptação das instituições e da legislação interna para cumprir as exigências de um texto que é de aplicação direta nos ordenamentos nacionais.[488]

Dado a similitude da regulação europeia com a proposta regulatória brasileira, veremos a partir de agora em maiores detalhes como se manifesta cada um dos princípios previstos no PL 5276.

O primeiro dos princípios garantidos pelo PL consiste no *princípio da finalidade* (art. 6º, I), exigindo que o destino a ser conferido aos dados deve ser informado previamente[489] aos usuários e que os dados colhidos só podem ser utilizados para fins legítimos. Veda-se, ainda, a transferência de dados pessoais a terceiros.

[487] Disponível em: <http://www.altitudesoft.com.br/sobre-nos/centro-de-noticias/articles/altitude-software-promoveu-debate-sobre-gdpr-no-porto/2584>. Acesso em: 27 mar. 2017.
[488] Disponível em: < http://www.callcentermagazine.net/contact-centers/altitude-software-discute-novo-regulamento-da-protecao-dados/>. Acesso em: 27 mar. 2017.
[489] Note que há críticos à necessidade de que as empresas avisem previamente aos usuários toda a vez que forem colher determinado dado: "With respect to notice and choice, some participants expressed concern about its feasibility, given the ubiquity of IoT devices and the persistent and pervasive nature of the information collection that they make possible. As one participant observed, when a bunch of different sensors on a bunch of different devices, on your home, your car, your body . . . are measuring all sorts of things, it would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported. Another participant talked about the risk that, if patients have to consent to everything for a health monitoring app, patients will throw the bloody thing away. Yet another participant noted that any requirement to obtain consent could be a barrier to socially beneficial uses of information." (FEDERAL TRADE COMISSION. Internet of things: Privacy & Security in a Connected World. FTC Staff Report, 2015, p. 21-22).

A partir deste princípio pode-se estruturar "um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)".[490] Durante a Consulta Pública realizada a respeito do anteprojeto de lei de proteção de dados pessoais, foram sugeridas alterações quanto ao princípio da finalidade. Todas concordavam que deveria haver uma flexibilização do princípio e que não deveria haver a qualificação de finalidades *específicas, explícitas e conhecidas*. Contudo, a nova adjetivação é controversa: alguns, como a CNseg e a ABRANET, entendem que devem se tratar de finalidades *devidamente informadas*; outros, como a CNI e a Febrabam, finalidades *esperadas*; por fim, a MPA sugeriu que o princípio da finalidade deve ter uma exceção para combate à fraude e atividades ilegais praticadas na Internet[491].

Pelo *princípio da adequação* (art. 6º, II), os dados coletados devem ser usados apenas na medida em que for necessário para atingir os objetivos anteriormente informados e de acordo com as legítimas expectativas do titular. Neste ponto, é necessário especificar o conceito de *legítimas expectativas*.

Para o Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal (SindiTeleBrasil), por exemplo, é preciso haver associação entre a expectativa do titular e o consentimento por ele dado ao responsável pelo tratamento[492]. Confira-se a posição adotada pelo *Centre for Information Policy Leadership*: [493]

> Para garantir a correta interpretação do que é uma finalidade compatível, é recomendável incluir algumas orientações adicionais sobre os fatores que os responsáveis devem levar em conta ao determinar se uma finalidade posterior é compatível ou não. Este é o tratamento adotado na Europa.

Apenas os dados indispensáveis para atingir a finalidade podem ser coletados, como indica o *princípio da necessidade* (art. 6º, III). É imprescindível que haja, sempre, a indagação do porquê é necessário coletar determinados dados,

[490] BRASIL. Escola Nacional de Defesa do Consumidor. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010, p. 46.
[491] INTERNET LAB. *O que está em jogo no debate sobre dados pessoais no Brasil?* (Relatório Final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de Proteção de Dados Pessoais), 2016, p. 78-79.
[492] Ibid, p. 80.
[493] Ibid, p. 81.

devendo a resposta ser a mais clara possível. Em suma, somente o mínimo necessário para a realização das finalidades deve ser colhido – o que está ligado, também, à segurança dos dados, pois, como observa o Instituto Brasileiro de Defesa do Consumidor (Idec), a grande quantidade de dados aumenta o interesse de hackers e ladrões pelas informações colhidas: [494]

> Um grande conjunto de dados coletados por tais dispositivos gera incentivos para ataques hackers e ladrões, *dentro e fora das empresas*. Qualquer política pública formulada sobre esse setor deve ter em mente um conjunto de medidas regulatórias para (i) incentivar o uso mínimo de dados pessoais e (ii) desincentivar o uso desproporcional de dados, violando os princípios da futura lei geral de proteção de dados pessoais.

Note-se que quanto maior a quantidade de objetos inteligentes, maior a probabilidade de ataques e abusos ocorrerem[495]. Nada obstante a importância deste princípio, há quem defenda uma aplicação minorada no que se refere à *IoT*, uma vez que limitar os dados que podem ser colhidos criaria, por exemplo, dificuldades à inovação tecnológica[496].

Além disso, o *princípio do livre acesso* (art. 6º, IV) assegura que as pessoas possam ter acesso aos próprios dados no momento em que desejarem. Garante-se, assim, o direito à consulta facilitada e gratuita sobre os dados coletados e o tratamento a eles dispensado. Após a consulta, e tendo por base o princípio da qualidade, que será visto a seguir, é possível retificar informações

---

[494] ZANATTA, Rafael A. F. *Internet das Coisas:* privacidade e segurança na perspectiva dos consumidores [Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017] – Instituto Brasileiro de Defesa do Consumidor, 2017, p. 5.

[495] FEDERAL TRADE COMISSION. *Internet of things: Privacy & Security in a Connected World*. FTC Staff Report, 2015, p. 12.

[496] Foi o que notou o Federal Trade Comission em seu relatório: With respect to data minimization – which refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it – one participant expressed concerns that requiring fledgling companies to predict what data they should minimize would "chok[e] off potential benefits and innovation." A second participant cautioned that "[r]estricting data collection with rules like data minimization could severely limit the potential opportunities of the Internet of Things" based on beneficial uses that could be found for previously-collected data that were not contemplated at the time of collection. Still another participant noted that "[d]ata-driven innovation, in many ways, challenges many interpretations of data minimization where data purpose specification and use limitation are overly rigid or prescriptive." (FEDERAL TRADE COMISSION. *Internet of things:* Privacy & Security in a Connected World. FTC Staff Report, 2015, p. 21)

incorretas, cancelar aquelas registradas de forma indevida, suprimir as obsoletas ou impertinentes e, até mesmo, realizar acréscimos[497].

Para a Febraban, não deveria ser assegurada consulta facilitada sobre as modalidades de tratamento de dados, pois isto não traria benefícios aos usuários e a modalidade deve ficar a critério do responsável, podendo configurar estratégia empresarial[498].

O *princípio da qualidade dos dados* (art. 6º, V) requer que os dados colhidos sejam verídicos e que correspondam, de fato, à forma como a pessoa utilizou os objetos e interagiu com a tecnologia. Ainda, exige que tais dados estejam atualizados.

Em outras palavras, "os dados armazenados devem ser fieis à realidade, atualizados, completos e relevantes", e, para isto, é preciso que a coleta e o tratamento dos dados "sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade"[499].

Neste ponto, há debate quanto à responsabilidade das empresas pela exatidão, clareza e atualização dos dados pessoais. Para alguns, esta responsabilidade não deveria existir; para outros, deveria ser limitada ao oferecimento de mecanismos para que os próprios titulares efetuem as atualizações e não haveria responsabilidade no caso de desconhecimento da desatualização; há, ainda, a posição de que a responsabilidade deva se limitar à manutenção e atualização, excluída a hipótese de erro, culpa ou dolo do titular dos dados; e a de que a responsabilidade deve ser conferida ao titular dos dados pessoais[500].

O *princípio da transparência* (art. 6º, VI) indica que informações sobre a finalidade que está sendo destinada aos dados, o tratamento a eles despendido e os agentes de tratamento devem ser claros e acessíveis aos usuários. Com tal

[497] BRASIL. Escola Nacional de Defesa do Consumidor. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010, p. 46.
[498] INTERNET LAB. *O que está em jogo no debate sobre dados pessoais no Brasil?* (Relatório Final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de Proteção de Dados Pessoais), 2016, p. 82-83.
[499] BRASIL. Escola Nacional de Defesa do Consumidor. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010, p. 46.
[500] INTERNET LAB. *O que está em jogo no debate sobre dados pessoais no Brasil?* (Relatório Final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de Proteção de Dados Pessoais), 2016, p. 83-84.

princípio, que também se aplica à Administração Pública, confere-se ao cidadão o poder de autodeterminação, pois, tendo conhecimento da finalidade de seus dados, pode o usuário definir o que será feio com eles.

Pelo *princípio da segurança* (art. 6º, VII), quanto mais íntimos forem os dados, maior deve ser a capacidade técnica utilizada. Vale dizer, a tecnicidade deve ser proporcional à natureza dos dados. Ademais, as medidas técnicas e administrativas devem ser sempre atualizadas e hábeis a proteger os dados de acessos não autorizados, de acidentes e de situações "ilícitas de destruição, perda, alteração, comunicação ou difusão".

Para o Instituto Brasileiro de Defesa do Consumidor, as empresas devem disponibilizar em seus sítios eletrônicos, no caso de dispositivos com interface de uso, informações sobre os padrões de segurança por elas adotados, e por meio de envio físico e da publicidade em lojas, no caso de dispositivos sem interface de uso[501].

Apesar de já existirem riscos à segurança em computadores e redes tradicionais, eles são aumentados na IoT. Tais riscos são: "(1) *permitindo o acesso não autorizado e uso indevido de informações pessoais; (2) facilitando ataques a outros sistemas; e (3) criando riscos de segurança ".*[502] Os princípios de segurança também devem ser aplicados quando da elaboração do design dos objetos, como se verá adiante:[503]

> Um participante descreveu como ele conseguiu *hackear* remotamente duas bombas de insulina conectadas e alterar as configurações para que elas não mais entregassem remédio. Outro participante falou sobre um conjunto de experimentos em que um invasor poderia obter "acesso à rede interna de computadores de um carro sem tocar fisicamente no carro". Ele descreveu como ele conseguiu invadir a unidade telemática interna de um carro e controlar o motor do veículo, ressaltando, no entanto, que "o risco para os proprietários de

[501] ZANATTA, Rafael A. F. *Internet das Coisas*: privacidade e segurança na perspectiva dos consumidores [Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017] – Instituto Brasileiro de Defesa do Consumidor, 2017, p. 9.

[502] FEDERAL TRADE COMISSION. *Internet of things:* Privacy & Security in a Connected World. FTC Staff Report, 2015, p. 10.

[503] Embora os riscos atualmente possam ser pequenos, eles tendem a se amplificar conforme a IoT avança. Por exemplo, o acesso não autorizado a câmeras ou monitores conectados à Internet levanta preocupações potenciais de segurança física. Do mesmo modo, o acesso não autorizado a dados recolhidos por dispositivos de fitness e outros dispositivos que rastreiam a localização dos consumidores ao longo do tempo podem pôr em perigo a segurança física dos consumidores. Outra possibilidade é que um ladrão possa acessar remotamente dados sobre o consumo de energia de contadores inteligentes para determinar se um proprietário está fora de casa, entre diversos outros exemplos.

> automóveis hoje é incrivelmente pequeno", em parte porque "todos os fabricantes de automóveis que conheço estão proativamente tentando resolver essas coisas". Embora os riscos atualmente possam ser pequenos, eles tendem a se amplificar conforme a IoT e uma vez que carros totalmente automatizados e outros objetos físicos automatizados, tornam-se mais prevalentes. O acesso não autorizado a câmeras conectadas à Internet ou monitores para bebês também levanta possíveis preocupações de segurança física. Do mesmo modo, o acesso não autorizado a dados coletados por dispositivos *fitness* e outros dispositivos que rastreiam a localização dos consumidores ao longo do tempo pode pôr em perigo a segurança física dos consumidores. Outra possibilidade é que um ladrão possa acessar remotamente dados sobre o uso de energia a partir de medidores inteligentes para determinar se um proprietário está longe de casa.[504][505]

Métodos preventivos com as medidas técnicas cabíveis devem ser adotados para evitar danos decorrentes do tratamento dos dados. É o que deriva do *princípio da prevenção* (art. 6º, VIII). Enquanto alguns defendem a supressão deste princípio, que seria abarcado pelo princípio da segurança, outros pontuam que sua definição legal deveria trazer um rol exemplificativo de boas práticas[506].

Por fim, os dados colhidos não podem ser manuseados de forma discriminatória nem para fins discriminatórios, o que é assegurado pelo *princípio da não discriminação* (art. 6º, XI).

Dados colhidos por meio da Internet das Coisas permitirão a classificação dos consumidores de uma forma extremamente precisa e jamais feita antes. Tal classificação pode levar a indesejáveis formas de discriminação. Como

[504] FEDERAL TRADE COMISSION. Internet of things: Privacy & Security in a Connected World. FTC Staff Report, 2015, p. 13.

[505] Tradução livre do autor. No original: *One participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine. Another participant discussed a set of experiments where an attacker could gain "access to the car's internal computer network without ever physically touching the car." He described how he was able to hack into a car's built-in telematics unit and control the vehicle's engine and braking, although he noted that "the risk to car owners today is incredibly small," in part because "all the automotive manufacturers that I know of are proactively trying to address these things." Although the risks currently may be small, they could be amplified as fully automated cars, and other automated physical objects, become more prevalent. Unauthorized access to Internet-connected cameras or baby monitors also raises potential physical safety concerns. Likewise, unauthorized access to data collected by fitness and other devices that track consumers' location over time could endanger consumers' physical safety. Another possibility is that a thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home.*

[506] INTERNET LAB. *O que está em jogo no debate sobre dados pessoais no Brasil?* (Relatório Final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de Proteção de Dados Pessoais), 2016, p. 88.

exemplifica Scott Peppet, empregadores podem avaliar os dados de candidatos a fim de decidir qual deles contratar[507].

O autor faz uma previsão de que, apesar de, inicialmente, não parecer, *tudo revela tudo* (*everything reveals everything*). Explica-se. Apesar de, aparentemente, informações colhidas de dispositivos de saúde não revelarem a capacidade de crédito, por exemplo, há razões para termos preocupações. Isto por dois motivos. O primeiro é baseado no *sensor fusion*, uma técnica pela qual dados obtidos de diferentes dispositivos são cruzados, gerando um resultado melhor do que se os dados fossem usados separadamente:[508]

> O princípio *sensor fusion* significa que os dados recolhidos a partir de vários sensores pequenos podem ser combinados para fazer mais inferências complexas do que se poderia esperar. Os dados de um acelerômetro e um giroscópio – ambos medidores de movimentos simples – podem ser combinados para inferir o nível de relaxamento de uma pessoa (com base em se os seus movimentos são constantes ou mesmo se são instáveis e tensos). Se acrescentarmos os dados do sensor de frequência cardíaca, pode-se facilmente inferir os níveis de estresse e emoções, porque estudos mostraram que as variações de frequência cardíaca em razão de exercício físico têm um padrão diferente do que aumentos devidos à excitação ou emoção. De modo semelhante, podem-se inferir emoções ou estados mentais a partir de uma variedade de outras atividades diárias, tais como a forma que um consumidor segura um telefone celular, o quão suavemente a pessoa digita uma mensagem de texto, ou o quão instável as mãos de uma pessoa são, enquanto seguram seu telefone. Novamente, a fusão de sensores permite que inferências complexas e inesperadas sejam extraídas de fontes de dados aparentemente simples. Como os consumidores usam dispositivos com muitos e diferentes tipos de sensores – desde rastreadores de *fitness* a automóveis, fornos a crachás de identificação no local de trabalho – estes sensores de dados irão se fundir para revelar mais coisas diferentes sobre os comportamentos, hábitos e intenções futuras dos indivíduos.[509]

---

[507] PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, v. 93, p. 117-120, 2014.

[508] Tradução livre do autor. No original: *The principle of sensor fusion means that data gleaned from various small sensors can be combined to draw much more complex inferences than one might expect. Data from an accelerometer and a gyroscope—both of which measure simple movements—can be combined to infer a person's level of relaxation (based on whether their movements are steady and even or shaky and tense). If one adds heart-rate sensor data, one can readily infer stress levels and emotions, because research has shown that heart-rate variations from physical exercise have a different pattern than increases due to excitation or emotion. Similarly, one might infer emotion or mental state from a variety of other daily activities, such as the way a consumer holds a cell phone, how smoothly a person types a text message, or how shaky a person's hands are while holding their phone. Again, sensor fusion allows such complex and unexpected inferences to be drawn from seemingly simple data sources. As consumers use devices with more and different types of sensors—from fitness trackers to automobiles, ovens to workplace identification badges—these sensor data will fuse to reveal more and different things about individuals' behaviors, habits, and future intentions.*

[509] PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, v. 93, p. 121-, 2014.

O segundo motivo, baseia-se na ideia de *Big Data*: os dispositivos podem colher informações físicas e fisiológicas sobre seus usuários e, com a aplicação de algoritmos[510] a estes dados, é possível fazer inferências sobre o estado físico, fisiológico e comportamental das pessoas. Confira-se:[511]

> Seguindo com essa busca de fontes de dados mais preditivo e com maiores nuances, os credores estão começando a experimentar a incorporação de dados de sensores de Internet de Coisas em tais decisões. Dados de telefone celular são um primeiro lugar óbvio para começar. Por exemplo, Safaricom, a maior operadora de telefonia celular do Quênia, estuda seus usuários de telefones celulares para estabelecer sua confiabilidade. Com base na frequência com que seus clientes completam seu tempo de antena, por exemplo, ela pode então decidir estender seu crédito. De forma semelhante, a Cignifi usa o comprimento, a hora do dia e a localização das chamadas de celular para inferir o estilo de vida dos usuários de *smartphones* – e, portanto, a confiabilidade desses usuários – para os candidatos a empréstimos no mundo em desenvolvimento.[512]

Com todos esses métodos de coleta e cruzamento de dados, formas obscuras de discriminação por raça, idade, gênero ou condição social, por exemplo, podem surgir, de modo que é necessário a previsão legal do princípio da não discriminação. Além disso, cabe lembrar que a própria Constituição Federal de 1988 prevê a proibição de discriminação[513].

Diante disto, é de extrema urgência a aprovação de uma lei de proteção aos dados pessoais[514] e a aplicação efetiva da lei por parte de empresas e da Administração Pública. A existência de incontáveis dispositivos que utilizam a

---

[510] Sobre os riscos derivados do uso de algorítimos, como manipulação, discriminação social e violações de privacidade, v. DONEDA, Danilo; ALMEIDA, Virgilio A. F. What is Algotihm Governance? *IEEE Internet Computing*, p. 2-5, jul./ago. 2016. Os autores consideram a necessidade de um processo de *algorithm governance* para evitar a concretização desses riscos.

[511] Tradução livre do autor. No original: *In keeping with this search for more nuanced and predictive data sources, lenders are beginning to experiment with incorporating Internet of Things sensor data into such decisions. Cell-phone data are an obvious first place to start. For example, Safaricom, Kenya's largest cell-phone operator, studies its mobile phone users to establish their trustworthiness. Based on how often its customers top up their airtime, for example, it may then decide to extend them credit.237 Similarly, Cignifi uses the length, time of day, and location of cell calls to infer the lifestyle of smartphone users—and hence the reliability of those users—for loan applicants in the developing world*.

[512] PEPPET, Scott R. op.cit, p. 122-123, 2014.

[513] Constituição Federal de 1988, Art. 3º "Constituem objetivos fundamentais da República Federativa do Brasil: (...) IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação." "Art. 5º (...) XLI - a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais;"

[514] Conforme sustentado anteriormente, A necessidade de uma lei geral de proteção dos dados pessoais se justifica pelo fato de ir além dos diplomas vigentes (como o Marco Civil da Internet, o CDC, a Constituição e o Código Civil), sendo especificamente voltada para coibir abusos relacionados aos dados pessoais, bem como pelo fato de trazer definições conceituais e técnicas importantes como, por exemplo, sobre "dados sensíveis", entre outros conceitos relevantes.

tecnologia da IoT, põe em evidência o direito de "proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços perigosos ou nocivos"[515-516]. Apesar de ainda ser discutível a necessidade de termos uma lei específica para tratar da IoT – a tecnologia ainda está em desenvolvimento e legislar sobre o tema agora seria prematuro sem um amplo debate ético na esfera pública – é de suma importância a elaboração de uma lei geral de proteção de dados pessoais[517].

Com a lei não se objetiva frear inovações tecnológicas. O PL nº 5276/2015 está, na verdade, em consonância com outras normas protetivas aos dados pessoais no cenário internacional[518]. Ao mesmo tempo em que é preciso assegurar o desenvolvimento da tecnologia, deve-se garantir a seus usuários que sua privacidade estará resguardada, o que é feito, por exemplo, por meio de princípios previstos na lei que norteiem a atividade empresarial.

Assim, a lei deve acompanhar ao máximo as inovações tecnológicas que surgirão com o tempo. A fluidez necessária para evitar a obsolescência da lei é exposta, por exemplo, no art. 6º, VII que, ao prever o princípio da segurança, não especifica de forma literal ou taxativa as obrigações dos agentes de segurança, mas as identifica através do resultado esperado.

Isto ocorre "pela dificuldade e mesmo pelo não cabimento de abordar diretamente em um documento normativo práticas de segurança que, para que sejam realmente atuais e eficazes, são fluidas e costumam mudar e se atualizar

[515] Código de Defesa do Consumidor, art. 6º, I.
[516] ZANATTA, Rafael A. F. Internet das Coisas: privacidade e segurança na perspectiva dos consumidores [Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017] – *Instituto Brasileiro de Defesa do Consumidor*, 2017, p. 4.
[517] FEDERAL TRADE COMISSION. Internet of things: Privacy & Security in a Connected World. FTC Staff Report, 2015, p. 49.
[518] Neste sentido, ZANATTA, Rafael A. F. Internet das Coisas: privacidade e segurança na perspectiva dos consumidores [Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017] – Instituto Brasileiro de Defesa do Consumidor, 2017, p. 12: "É importante lembrar que os princípios gerais do PL 5276/15 não diferem muito dos *Fair Principles* adotados nos Estados Unidos da América em 1973 e dos princípios presentes na nova Diretiva de Proteção de Dados Pessoais do Parlamento Europeu, baseados nos princípios da OCDE de 1980 e na Diretiva de 1995. Assim, a garantia da moldura jurídica construída no PL 5276/15 não configura obstáculo à inovação, estando bastante alinhada com os desenvolvimentos jurídicos recentes.".

constantemente" [519]. Caso a especificação seja necessária, órgão competente poderá fazê-lo, como autorizado pelo art. 45, § 1º do projeto[520].

Nada obstante, o desenvolvimento da indústria relacionada à *IoT* sem a aprovação de uma lei de proteção de dados pessoais "é extremamente danosa"[521].

Diversas Organizações Não Governamentais juntaram-se para manifestar seu apoio à aprovação do PL nº 5276/2016, publicando uma carta aberta[522]. As entidades pontuaram o modo colaborativo pelo qual foi elaborado o projeto, contando com amplo engajamento social por meio de consultas públicas, e o seu rigor técnico-normativo [523]. O projeto, assim, supriria "grave lacuna no ordenamento jurídico brasileiro, a ponto de trazer segurança jurídica para o cidadão, para a atividade empresarial e para a administração pública no tratamento dos dados pessoais".

Ao mesmo tempo em que assegura direitos e garantias ao cidadão sobre seus dados, o projeto prevê regras e limites para que os setores privado e público utilizem esses dados, trazendo grande segurança jurídica e atendendo a demandas duplas: [524]

[519] MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista de Direito Civil Contemporâneo*, São Paulo, v. 9, p. 35-48, out./dez. 2016, p. 44.

[520] Art. 45. "O operador deve adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º O órgão competente poderá dispor sobre padrões técnicos e organizacionais para tornar aplicável o disposto no *caput*, levando-se em consideração a natureza das informações tratadas, características específicas do tratamento e o estado atual da tecnologia, em particular no caso de dados sensíveis".

[521] ZANATTA, Rafael A. F. Internet das Coisas: privacidade e segurança na perspectiva dos consumidores [Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017] – Instituto Brasileiro de Defesa do Consumidor, 2017, p. 5.

[522] Disponível em: http://www.idec.org.br/pdf/carta-aberta-pl-dados-pessoais-jun2016.pdf.

[523] Além de destacar a previsão de criação de um órgão de fiscalização, afirmou-se na carta que o PL "Sistematiza de maneira orgânica os conceitos e princípios de proteção de dados pessoais, delimitando de maneira clara seu escopo de aplicação e os critérios interpretativos necessários para a sua aplicação, abordando dentre outros pontos: i) os direitos dos cidadãos de acesso, retificação, correção e oposição ao tratamento de seus dados pessoais; ii) regras que vão do início ao término da atividade de tratamento de dados pessoais, bem como a respeito da responsabilidade civil de toda a cadeia de agentes nela inserida; iii) a criação de um capítulo específico para a proteção dos dados pessoais do cidadão frente ao Poder Público, havendo, assim, simetria regulatória entre os setores privado e público; iv)a regulação da transferência internacional dos dados pessoais, reconhecendo a necessária proteção dos dados pessoais em uma cenário transfronteiriço; v) mecanismos de incentivo para o setor regulado, dedicando um capítulo específico para boas práticas"

[524] MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista de Direito Civil Contemporâneo*, São Paulo, v. 9, p. 35-48, out./dez. 2016, p. 48.

> Por um lado, com a atualização da proteção da privacidade de forma que o brasileiro possa gozar efetivamente de uma cidadania digital, e, por outro, por meio da criação de um espaço favorável para a inovação e utilização de dados pessoais dentro de um ambiente de legitimidade e de respeito às escolhas fundamentais do cidadão.

É preciso dar atenção aos mínimos detalhes dessa lei, pois ela terá grande impacto social. Assim, deve-se elencar princípios que norteiem a atividade empresarial, protegendo os dados pessoais dos cidadãos e assegurando efetividade ao direito à privacidade.

Há outros pontos importantes de conexão, como a previsão sobre acesso facilitado às informações sobre o tratamento dos dados pessoais pelo titular. Pelo PL, as informações devem ser disponibilizadas de forma clara, adequada e ostensiva sobre, dentre outros aspectos, a finalidade do tratamento, sua forma e duração (art. 8º). Similar a este regramento, o art. 12 da GDPR trata da transparência e de regras para o exercício dos direitos dos titulares dos dados, ao passo que o art. 13 aborda a informação e o acesso aos dados pessoais.

A definição de dados pessoais é muito similar nos dois diplomas ora analisados, como se pode perceber dos dispositivos abaixo transcritos e na tabela abaixo:

> PL nº 5276/2016, Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;

> GDPR, Artigo 4.º Definições Para efeitos do presente regulamento, entende-se por: 1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

As definições de dados pessoais sensíveis também são próximas. A GDPR prevê o conceito no art. 9º[525] e no preâmbulo (itens 10 e 51), ao passo que o PL o

[525] Artigo 9.º *Tratamento de categorias especiais de dados pessoais* 1.É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

faz no art. 5º, inciso III[526]. Da mesma forma, o tratamento destinado a estes dados é semelhante: veda-se, como regra, o uso de dados sensíveis, havendo algumas exceções em cada diploma[527].

Um ponto interessante de distinção entre as duas regulações diz respeito ao tratamento de dados pessoais de crianças e adolescentes. O PL prevê que tal tratamento "deverá ser realizado no seu melhor interesse, nos termos da legislação pertinente" (art. 14)[528]-[529], ao passo que a GDPR traz previsão sobre as condições aplicáveis ao consentimento de crianças no art. 8º.

A partir de 16 anos, pode a criança manifestar consentimento; abaixo desta idade, o tratamento de dados só será lícito "se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança".

Em relação às sanções por descumprimento da lei, também há semelhanças e diferenças entre a regulação brasileira e a europeia. Aquela prevê outros tipos de sanção além da multa, apesar de a GDPR abrir a possibilidade para que Estados-Membros criem novas formas de punição.

Na Europa, porém, há limites claros de valor para a multa, diferente do Brasil. A regulação europeia prevê a aplicação de multas para o seu descumprimento, que serão asseguradas por cada autoridade de controle, como previsto no art. 83 da GDPR. A lei trata dos limites da multa, cujo valor varia de acordo com a natureza, gravidade e duração da infração, dentre outros aspectos. Outras sanções podem ser aplicadas em relação às violações não sujeitas a multa. Cabe aos Estados-Membros estabelecer as regras neste âmbito.

---

[526] Art. 5º. Para os fins desta Lei, considera-se: III - dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos;

[527] Confira-se o art. 11 do PL nº 5276/2016 e o art. 9º da GDPR.

[528] Note-se que o art. 28, § 1º do Estatuto da Criança e do Adolescente prevê que em processos de colocação em família substituta, a criança e o adolescente devem, sempre que possível, serem previamente ouvidos. No caso de maiores de 12 anos, é preciso da manifestação do consentimento (art. 28, § 2º). A necessidade de oitiva pode se aplicar, por analogia, a outros procedimentos que afetam as crianças e adolescentes e é uma opção de interpretação que pode ser adotada no tema do tratamento de dados. Sobre a discussão entre autonomia e proteção de crianças e adolescentes, confira-se o estudo da professora do Departamento de Psicologia da PUC-Rio ARANTES, Esther Maria de Magalhães. Proteção Integral à Criança e ao Adolescente: Proteção *versus* Autonomia. *Psicologia Clínica*, n. 2, v. 21, p. 431-450, 2009.

[529] Sobre o princípio do melhor interesse da criança, confira-se MEIRELLES, Rose Melo Vencelau. O Princípio do Melhor Interesse da Criança. In: MORAES, Maria Celina Bodin (Coord.). *Princípios do Direito Civil Contemporâneo*. Rio de Janeiro: Renovar, 2006, p. 459-493.

O PL nº 5276/2016 prevê como sanções - que podem ser aplicadas isolada ou cumulativamente - às pessoas jurídicas de direito privado que desrespeitarem as normas legais a (i) multa; (ii) publicização da infração; (iii) anonimização dos dados pessoais; (iv) bloqueio dos dados pessoais; (v) suspensão de operação de tratamento de dados pessoais; (vi) cancelamento dos dados pessoais e (vii) suspensão de funcionamento de banco de dados. Os itens (iii) a (vii) podem ser aplicados às entidades e aos órgãos públicos. Sanções previstas em legislação específica não são substituídas pelas elencadas no PL.

Com base no exposto, resta clara a forte influência da regulação europeia sobre a proposta de regulação no Brasil. Exploraremos, a seguir, algumas especificidades da normativa europeia tendo em vista tanto seus reflexos nas proposições brasileiras quanto sua aplicabilidade direta a empresas (ainda que nacionais) que processem dados de cidadãos europeus.

2.4.1
Especificidades da Regulação Europeia

A proteção da privacidade em países europeus possui notória importância. Na década de 1970, por exemplo, foi publicada a primeira lei de proteção de dados na Alemanha[530]. A Carta de Direitos Fundamentais da União Europeia protege, no artigo 7º, a vida privada e, no artigo 8º, prevê a proteção aos dados pessoais. Também o Tratado de Lisboa[531], o Tratado sobre o Funcionamento da União Europeia[532], o Tratado que estabelece uma Constituição para a Europa[533] e a Carta dos direitos fundamentais da União Europeia[534] asseguram esta proteção.

---

[530] FORTES, Vinicius Borges. *Os direitos de privacidade e a proteção de dados pessoais na Internet*. Rio de Janeiro: Lumen Juris, 2016, p. 153-154.

[531] ARTIGO 39.º Em conformidade com o artigo 16.º do Tratado sobre o Funcionamento da União Europeia e em derrogação do n.º 2 do mesmo artigo, o Conselho adopta uma decisão que estabeleça as normas relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados- -Membros no exercício de actividades relativas à aplicação do presente capítulo, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes.

[532] Artigo 16.º (ex-artigo 286.o TCE)

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre

Na Europa, a *General Data Protection Regulation* (GDPR) (Regulamento (UE) 2016/679), que será aplicável a partir de 25 de maio de 2018, veio para fazer uma revisão da legislação europeia acerca da proteção de dados e, assim, substitui a Diretiva de Proteção de Dados de 1995 (95/46/EC). Ela se aplica a todos os 28 países da União Europeia (UE) e integra um pacote de mudanças que inclui uma nova Diretiva de Proteção de Dados para os setores de polícia e de justiça criminal[535].

Em 2009, a Comissão Europeia percebeu que, devido ao rápido avanço da tecnologia, era necessário alterar a regulamentação existente. Desta forma, iniciou estudos que se focavam (i) nos impactos das novas tecnologias; (ii) na falta de harmonia entre os Estados Membros; (iii) na globalização e na internacionalização das transferências de dados; (iv) na necessidade de garantir cumprimento efetivo e (v) na menor fragmentação dos instrumentos[536]. A GDPR foi proposta em 2012 pela Comissão Europeia e se seguiram quatro anos de intensas negociações entre o Parlamento Europeu e o Conselho da União Europeia, até que, em abril de 2016, a versão final foi publicada[537].

Dentre os agentes que devem observar os dispositivos da GDPR, estão as empresas que oferecem bens e serviços na União Europeia que lidem com dados pessoais de residentes na UE[538]. Tais empresas devem ser claras ao mostrar

---

circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes.

[533] Artigo I-51.o *Protecção de dados pessoais* 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. A lei ou lei-quadro europeia estabelece as normas relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de actividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes.

[534] Capítulo II, Artigo 8.° *Protecção de dados pessoais* 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[535] PROMONTORY. EU GDPR: A Primer. 19 fev. 2016. Disponível em: <http://www.promontory.com/News.aspx?id=4127>. Acesso em: 07 mar. 2017.

[536] ALVAREZ, Cecilia; BOWMAN, John; GERLACH, Natascha. Into The Unknown: The Proposed EU General Data Protection Regulation and Its Potential Effect On Transborder Data Flows. Digital Discovery & e-Evidence, 15 DDEE 286, set. 2015, p. 2.

[537] PROMONTORY. EU GDPR: Summary of Key Provisions. Disponível em: <http://www.promontory.com/uploadedFiles/Articles/Insights/151221_GDPR_compromise_A4.pdf>. Acesso em: 08 mar. 2017.

[538] O art. 3(2) especifica o âmbito de aplicação territorial: Art. 3º.2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um

porquê elas podem processar dados pessoais, devendo, dentre outras exigências, comprovar o consentimento livre, informado, específico e sem ambiguidade do usuário - e, em alguns casos, explícito.

A nova regulação prevê direitos aos sujeitos cujos dados são processados; disciplina obrigações de controladores e processadores de dados; revisa regras sobre transferência internacional de dados; estabelece multas; cria um regime regulatório transfronteiriço para a UE; e positiva novos direitos aos usuários, como o direito de acesso, o direito à portabilidade de dados e o direito ao esquecimento.

Antes de analisar a GDPR de forma pormenorizada, cabe apenas destacar que também há duas Diretivas que se destinam a proteger dados pessoais, mas possuem um âmbito de aplicação mais específico.

A Diretiva (UE) 2016/680 trata da "proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais".

Já a Diretiva (UE) 2016/681 é relativa à "utilização dos dados dos registros de identificação dos passageiros (PNR) para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave".

A GDPR, em seu Capítulo II, traz os princípios que devem ser observados pelos responsáveis pelo tratamento de dados pessoais[539]. Os princípios são: licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade, confidencialidade e responsabilidade. Estão dispostos no artigo 5º, da seguinte maneira:[540]

> **Princípios relativos ao tratamento de dados pessoais**
> 1. Os dados pessoais são:
> a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);
> b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o

responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União."

[539] Uma comparação entre os princípios previstos na legislação europeia e na legislação brasileira foi feito no tópico II.

[540] Disponível em: <https://www.eugdpr.org/>. Acesso em: 27 mar. 2017.

> tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»);
> c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);
> d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);
> e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);
> f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);
> 2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.o 1 e tem de poder comprová-lo («responsabilidade»).

O artigo 6º da GDPR traz as hipóteses em que o tratamento dos dados é lícito e elenca requisitos para tanto. É possível, porém, que haja processamento de dados sem se basear em consentimento para garantir determinados objetivos. Trata-se do *further processing*, que pode acontecer, por exemplo, para assegurar o interesse público no domínio da saúde pública. Em outras palavras, o item 4 trata da situação em que os dados foram utilizados para finalidades diferentes daquelas pelas quais fora recolhido e quando não houve consentimento do titular ou autorização legal para tanto.

O processamento não baseado em consentimento deve considerar a natureza dos dados pessoais, as possíveis consequências do processamento e a existência de garantias apropriadas. O responsável pelo tratamento dos dados só pode utilizá-los caso os fins para os quais deseja utilizar os dados seja compatível com a finalidade para a qual eles foram inicialmente recolhidos, devendo, para isso, ter em conta:[541]

> a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
> b) O contexto em que os dados pessoais foram recolhidos, em particular no

[541] Disponível em: <https://www.eugdpr.org/>. Acesso em: 27 mar. 2017.

> que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
> c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.o, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.o;
> d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;
> e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

A regra, no entanto, é que os dados sejam utilizados com o consentimento de seu titular - consentimento este que deve atender às exigências do artigo 7º, sendo, portanto, livre, prévio, renovável e expresso. Em geral, nos contratos em que o tratamento dos dados é apenas uma das prestações, a parte contratada deve explicitar de forma clara e simples para o titular quais dados serão tratados.

Interessante observar que, em regra, há dados que não podem sofrer tratamento por nenhuma pessoa ou entidade, como aqueles que revelem a origem racial ou étnica, as opiniões políticas ou dados biométricos que permitam identificar uma pessoa de forma inequívoca[542]. Há, entretanto, exceções a esta exclusão, previstas no item 2 do artigo 9º.

A GDPR possui um extenso capítulo tratando dos direitos do titular dos dados. Trata-se do capítulo III, do qual destacaremos alguns dispositivos que possuem maior relação com a privacidade e com a inovação.

O Capítulo inicia-se pontuando a necessidade de se assegurar a transparência das informações, das comunicações e das regras para o exercício dos direitos dos titulares dos dados. Neste sentido, o responsável pelo tratamento deve fornecer informações concisas, transparentes, inteligíveis, de fácil acesso e com linguagem clara e simples. As regras sobre como as informações devem ser prestadas e sobre como o titular pode requerê-las estão dispostas no artigo 12º.

De modo geral, quando os dados são recolhidos junto do titular, o responsável pelo tratamento deve disponibilizar meios para própria identificação (identidade, contatos, etc.), as finalidades do tratamento dos dados, o seu

[542] Confira o que prevê o item 1 do artigo 9º: 1.É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

fundamento jurídico, os destinatários ou as categorias de destinatários dos dados pessoais e seus interesses legítimos, conforme disposto no art. 13º da Lei.

Ademais, outras informações adicionais devem ser fornecidas quando necessário para garantir um tratamento equitativo e transparente, como prazo de conservação dos dados e o direito de apresentar reclamação a uma autoridade de controle.

O art. 13º trata de hipótese em que o tratamento dos dados se afasta das finalidades inicialmente informadas ao titular. Neste caso, é preciso fornecer informações sobre o fim e quaisquer outras informações pertinentes, como exige o art. 13(3).

Nada obstante, isto não se aplica quando o titular já tiver conhecimento das informações, o que pode gerar controvérsias sobre o que configura este conhecimento. Por exemplo, pode-se defender que a mera disposição destes elementos em um termo de uso é suficiente para afirmar que o titular possui conhecimento ou pode-se afirmar que é necessário haver manifestação inequívoca pelo titular de que ele está ciente do atual tratamento dos dados e das suas finalidades.

Quando os dados não são recolhidos junto do titular, as regras aplicáveis são as previstas no art. 14º. Similar a esta normatividade, temos, no PL brasileiro nº 5276/2016, o art. 8º que assegura o "acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva".

A Regulação europeia reconhece o direito de acesso do titular, que pode requerer confirmação de que seus dados pessoais estão ou não sendo tratados, de manifestar concordância com isto, além de obter informações sobre as finalidades do tratamento, as categorias dos dados, dentre outras (art. 15(1)). No caso de transferência internacional de dados ou para terceiros, o titular tem o direito de ser informado sobre as garantias adequadas (art. 15(2)).

Além de poder obter uma cópia dos dados que estão sendo tratados (art. 15(3)), o titular tem o direito de obter a retificação dos dados pessoais inexatos (art. 16).

Interessante previsão é a contida no art. 17º, que regula o direito ao esquecimento no cenário europeu. Em determinadas situações, pode o titular ter

seus dados apagados. Não se trata de uma vontade irrestrita do titular, mas limitada por condições específicas previstas na GDPR, a saber:[543]

> a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
> b) O titular retirar o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
> c) O titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 2;
> d) Os dados pessoais foram tratados ilicitamente;
> e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
> f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.o, n.o 1.

Além disso, há o direito à exclusão dos dados caso o responsável pelo tratamento tenha tornado-os públicos, situação em que se deve observar o item 2 do art. 17º:[544]

> 2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.o 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

Há casos, porém, em que os itens 1 e 2 não se aplicam. São situações em que os dados são necessários ao exercício da liberdade de expressão e de informação, ao cumprimento de obrigação legal, ao exercício de funções de interesse público ou ao exercício da autoridade pública investida do tratamento, por motivos de saúde pública, investigação científica, história ou para fins estatísticos e, ainda, para fins de declaração, exercício ou defesa de um direito em processo judicial. Todas as hipóteses estão previstas no art. 17(3).

O artigo 18 da GDPR traz o direito à limitação do tratamento. Assim, o tratamento de dados pode ser limitado por requerimento do titular quando se buscar contestar a exatidão dos dados, o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais, o responsável pelo tratamento já não

[543] Disponível em: <https://www.eugdpr.org>. Acesso em: 27 mar. 2017.
[544] Disponível em: <https://www.eugdpr.org>. Acesso em: 27 mar. 2017.

precisar dos dados para fins de tratamento ou quando o tratamento for oposto ao disposto no art. 21, parágrafo primeiro.

Nas operações de apagamento, retificação ou limitação de tratamento, o titular dos dados recebe uma notificação do responsável pelo tratamento avisando que a operação foi realizada. Dispensa-se a notificação apenas no caso de se demandar um esforço desproporcional por parte do responsável pelo tratamento.

O art. 20º prevê o direito de portabilidade dos dados, pelo qual o titular dos dados tem o direito de:[545]

> (...) 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.

Para isso, é preciso que o tratamento tenha se baseado no consentimento e que tenha sido realizado por meios automatizados.

O titular dos dados tem o direito de se opor, a qualquer momento, ao tratamento de dados que lhe digam respeito, incluindo a definição de perfis. O tratamento deve ser cessado, exceto se o responsável apresentar "razões imperiosas e legítimas" prevalecentes sobre interesses, direitos e liberdades do titular ou para efeitos de declaração, exercício ou defesa de um direito em processo judicial (art. 21(1)).

Na hipótese de dados tratados para efeitos de comercialização direta, porém, pode o titular se opor a qualquer momento ao tratamento dos dados para os efeitos da comercialização, de modo que os dados deixam de ser tratados para este fim (art. 21(2 e 3)).

No caso de dados utilizados para fins de investigação científica, história ou estatísticos, o titular também pode se opor, exceto se o tratamento for necessário para a prossecução de atribuições de interesse público (art. 21(6)).

Via de regra, o titular tem o direito de não se sujeitar a decisões tomadas exclusivamente com base em tratamento automatizado, incluindo a definição de perfis (art. 22), exceto se tiver dado consentimento explícito, se for autorizado por direito da União ou do Estado-Membro a que o responsável pelo tratamento

[545] Disponível em: <https://www.eugdpr.org>. Acesso em: 27 mar. 2017.

estiver sujeito ou se o processamento for necessário para a celebração ou execução de contrato entre o titular dos dados e o responsável por seu tratamento.

As decisões em comento, isto é, tomadas exclusivamente com base em tratamento automatizado, são realizadas por meio de *profiling*, técnica pela qual os dados coletados são utilizados para formar um perfil do usuário, como informa Danilo Doneda: [546]

> Nela [na técnica conhecida como profiling], os dados pessoais são tratados, com o auxílio de métodos estatísticos, técnicas de inteligência artificial e outras mais, com o fim de obter uma 'metainformação', que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destinos de uma pessoa ou grupo.

O perfil formado torna-se uma representação virtual da pessoa e pode até mesmo ser confundido com ela. A utilização da técnica, desta forma, pode diminuir a liberdade dos indivíduos, pois aqueles que se valem do perfil formado partem do pressuposto de que a pessoa tomará decisões com base em um padrão predefinido[547]. Por isso, de grande aplicabilidade prática será a previsão da GDPR acerca da possibilidade de que o usuário não se sujeite a decisões tomadas exclusivamente com base em *profiling*.

Apesar dos diversos direitos previstos na GDPR, e do avanço intrínseco à positivação, o art. 23 traz limitações que podem fragilizá-los. Os direitos e obrigações até aqui descritos podem ter seu alcance limitado por medida legislativa, desde que respeitada a essência dos direitos e liberdades fundamentais e desde que se trate de medida necessária e proporcional (art. 23º).

O Capítulo IV da GDPR trata do responsável pelo tratamento dos dados e do subcontratante, cabendo destacar alguns dispositivos específicos.

O art. 25 aborda a proteção de dados desde a concepção e por *default*, o que é conhecido internacionalmente pela expressão *data protection by design and default*. Deve o responsável pelo tratamento de dados adotar, tanto no momento de definição dos meios de tratamento como no do próprio tratamento, medidas técnicas e organizativas adequadas a fim de aplicar os princípios da proteção de dados de forma eficaz, incluindo também as garantias necessárias no tratamento.

[546] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 173.
[547] Ibid, p. 174.

Ainda, medidas devem ser aplicadas para garantir que, por *default* apenas dados pessoais necessários para cada finalidade específica do tratamento sejam tratados.

Pela proteção *by design*, entende-se que os princípios fundamentais de privacidade devem ser aplicados em todo o processo de desenvolvimento de um sistema[548]-[549]. Trata-se de conceito relativamente novo que está no centro dos debates sobre privacidade entre acadêmicos e legisladores[550].

Para Ann Cavoukian, Comissária de Informação e Privacidade de Ontário, província Canadense, de 1997 a 2014, o desafio consiste em transformar o conceito de *privacy by design* em ferramentas concretas:[551]

> Como demonstramos, a tarefa para os engenheiros e arquitetos de sistemas atentos à privacidade é traduzir a estrutura conceitual do PbD em um conjunto de ferramentas específicas e operacionalmente viáveis. Quando aplicadas por projetistas e gerentes de projeto, essas ferramentas garantirão que os requisitos de negócios, especificações de engenharia, metodologias de desenvolvimento, controles de segurança e as melhores práticas sejam desenvolvidas ou aplicadas de acordo com cada domínio ou escopo do projeto - com a privacidade como contexto.[552][553]

[548] Nas palavras de Jaap-Henk Hoepman, "The fundamental principle of privacy by design is, therefore, that privacy requirementsmust be addressed throughout the full system development process. In other words starting when the initial concepts and ideas for a new system are drafted, up to and including the final implementation of that system." HOEPMAN, Jaap-Henk. Privacy Design Strategies. In: CUPPENS-BOULAHIA, Nora et al. (Eds.). ICT Systems Security and Privacy Protection. New York: London, 2014, p. 446.

[549] Outra conceituação interessante é encontrada no sítio eletrônico da Regulação de Dados Pessoais da União Europeia: "In short, privacy by design means that each new service or business process that makes use of personal data must take the protection of such data into consideration. An organisation needs to be able to show that they have adequate security in place and that compliance is monitored. In practice this means that an IT department must take privacy into account during the whole life cycle of the system or process development.". Disponível em: <http://www.eudataprotectionregulation.com/data-protection-design-by-default>. Acesso em: 17 mar. 2017.

[550] KLITOU, Demetrius. *Privacy-Invading Technologies and Privacy by Design*: Safeguarding Privacy, Liberty and Security in the 21st Century. Berlin: Asser Press/Springer, 2014, p. 260.

[551] Tradução livre do autor. No original: *As we have demonstrated, the task for privacyaware engineers and systems architects is to translate the PbD conceptual framework into a set of specific, and operationally feasible, tools. When applied by designers and project managers, these tools will ensure that business requirements, engineering specifications, development methodologies, security controls and best practices will be developed or applied according to each domain or project scope – with privacy as the context*.

[552] CAVOUKIAN, Ann. Privacy by Design. IEEE Technology and Society Magazine, winter 2012, p. 19.

[553] Tradução livre do autor: Como demonstramos, a tarefa para engenheiros e arquitetos de sistemas de privacyaware é traduzir a estrutura conceitual PbD em um conjunto de ferramentas específicas e operacionalmente viáveis. Quando aplicados por designers e gerentes de projetos, essas ferramentas garantirão que os requisitos de negócios, especificações de engenharia, metodologias de desenvolvimento, controles de segurança e melhores práticas serão desenvolvidos ou aplicados de acordo com cada domínio ou âmbito do projeto - com privacidade como contexto.

Não há um modo de execução fixo pelo qual a proteção *by design* deve ser feita[554]. A fim de garantir a aplicação da ideia inerente a tal tipo de proteção, Jaap-Henk Hoepman elenca algumas estratégias de proteção da privacidade *by design* - algumas muito similares às previstas na GDPR. São elas: (i) *minimizar*, estratégia pela qual a quantidade de dados processados deve ser a mínima possível; (ii) *ocultar*, de modo que qualquer dado pessoal deve ser ocultado da *plain view*; (iii) *separar*, de forma que dados pessoais sejam processados em compartimentos separados sempre que possível; (iv) *agregar*, fazendo com que os dados pessoais sejam tratados ao mais alto nível de agregação e com o mínimo detalhe possível em que (ainda) seja útil; (v) *estratégias orientadas*, de modo que deve-se informar sempre que dados pessoais forem processados; (vi) *controle*, estratégia pela qual "*data subjects should be provided agency over the processing of their personal data*"; (vii) *enforce*, de forma que uma política de privacidade compatível com requisitos legais exista e seja aplicada e (viii) *demonstrar*, isto é, ser capaz de demonstrar conformidade com a política de privacidade de quaisquer requisitos legais[555].

Interessante observar que, a despeito do que possa parecer a primeiro plano, a proteção pelo design não impede a inovação. Pelo contrário. Neste sentido, Ann Cavoukian afirmou que proteger a privacidade demanda o mais alto nível de inovação[556].

No que tange à privacidade *by default*, confira-se:[557]

---

[554] KLITOU, Demetrius. *Privacy-Invading Technologies and Privacy by Design*: Safeguarding Privacy, Liberty and Security in the 21st Century. Berlin: Asser Press/Springer, 2014, p. 266.
[555] HOEPMAN, Jaap-Henk. Privacy Design Strategies. In: CUPPENS-BOULAHIA, Nora et al. (Eds.). *ICT Systems Security and Privacy Protection*. New York: London, 2014, p. 452-457.
[556] CAVOUKIAN, Ann. Privacy by Design. *IEEE Technology and Society Magazine*, winter 2012, p. 19.
[557] Tradução livre do autor. No original: *Privacy by Default simply means that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. There is also a temporal element to this principle, as personal information must by default only be kept for the amount of time necessary to provide the product or service. For example: imagine signing up for a new social media service on which you can share personal information, life events and other content you may deem relevant. In order to successfully publish your profile only your name and email address are required, yet the new service also automatically publishes your age and location and makes it available to the public rather than just to your connections. This would be a clear breach of the privacy by default principle as more information is disclosed to the public than is necessary to provide you with the service. It is noteworthy that the regulation specifically identifies and prohibits services that by default make personal information accessible to an indefinite number of individuals. This is a significant step in ensuring privacy on social media platforms and it is of particular importance to younger users.*

> Privacidade '*by default*', ou como regra, significa simplesmente que as configurações de privacidade mais estritas se aplicam automaticamente uma vez que um cliente adquire um novo produto ou serviço. Em outras palavras, nenhuma alteração manual das configurações de privacidade deve ser exigida por parte do usuário. Há também um elemento temporal sobre este princípio, uma vez que as informações pessoais devem, como padrão, apenas ser mantidas durante o período de tempo necessário para fornecer o produto ou serviço. Por exemplo: imagine se inscrever para um novo serviço de mídia social no qual você pode compartilhar informações pessoais, eventos da vida e outros conteúdos que você julgue relevantes. Para publicar o seu perfil com sucesso, basta o seu nome e endereço de e-mail, mas o novo serviço também publica automaticamente a sua idade e localização e os disponibiliza ao público em vez de apenas às suas conexões. Esta seria uma clara violação ao princípio da privacidade '*by default'*, uma vez que mais informação é revelada ao público do que é necessário para lhe fornecer o serviço. Vale ressaltar que o regulamento especificamente identifica e proíbe serviços que, por padrão, tornam informações pessoais acessíveis a um número indefinido de indivíduos. Este é um passo significativo para garantir a privacidade em plataformas de mídia social e é de particular importância para os usuários mais jovens.[558]

Especial atenção deve ser dispensada à Seção 2 do Capítulo IV, dedicada à segurança dos dados pessoais. O art. 32 preceitua que os responsáveis pelo tratamento e os subcontratantes devem aplicar as medidas técnicas e organizativas adequadas para garantir um nível de segurança adequado ao risco[559], o que inclui:

> a) A pseudonimização e a cifragem dos dados pessoais;
> b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
> c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
> d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

No caso de violação de dados pessoais, o art. 33 prevê o procedimento que deve ser adotado para comunicar o ocorrido à autoridade de controle. Quaisquer violações de dados pessoais devem ser documentadas pelo responsável pelo tratamento.

---

[558] Disponível em: <http://www.eudataprotectionregulation.com/data-protection-design-by-default>. Acesso em: 17 mar. 2017.

[559] O item 2 do art. 32 explicita quais são os riscos que devem ser levados em conta: "2.Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento."

O art. 34, por sua vez, prevê o procedimento para que, em caso de violação de dados pessoais suscetível de implicar elevado risco para os direitos e liberdades das pessoas singulares, a comunicação seja feita ao titular dos dados.

A Seção 3 disciplina a avaliação de impacto sobre a proteção de dados e a consulta prévia. A avaliação de impacto deve ser realizada sempre que um novo tratamento - sobretudo os que usem novas tecnologias e tendo em vista sua natureza, âmbito, contexto e finalidades - for capaz de implicar elevado risco para os direitos e liberdades das pessoas singulares.

A avaliação, cujo conteúdo mínimo foi positivado no item 7[560], deve ser realizada antes de o tratamento ser iniciado. Nos casos elencados no item 3 do art. 35 e reproduzidos a seguir, a avaliação é obrigatória:

> a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
> b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o; ou
> c) Controlo sistemático de zonas acessíveis ao público em grande escala.

O Capítulo V trata especificamente da transferência internacional de dados - para países terceiros ou para organizações internacionais. As regras ali previstas não mudaram de forma substancial em relação à Diretiva 95/46/EC.

A GDPR previu o sistema chamado *one-stop shop*, pilar central da nova regulação criada. Uma autoridade principal regula controladores de dados e, caso uma autoridade de supervisão conteste aquela, será dada uma decisão pelo Conselho Europeu de Proteção de Dados (EDPB, na sigla em inglês), podendo haver apelação para a Corte de Justiça da União Europeia[561]-[562].

---

[560] Art. 35(7).A avaliação inclui, pelo menos: a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento; b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos; c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.o 1; e d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

[561] Sobre o tema, confira-se o Capítulo VI da GDPR, que trata sobre autoridades de controle independentes.

[562] Os itens 127 e 128 do preâmbulo trazem uma explicação sobre o assunto. Confira-se:

Por fim, outra diretriz importante diz respeito à autoridade de supervisão que deve ser notificada pelos controladores em casos de violação de dados pessoais. Além disso, controladores e processadores devem designar um responsável pela proteção de dados (*Data Protection Officers - DPO*), que age de forma independente daqueles e cujas atividades principais consistem em regular e realizar sistemático monitoramento de dados pessoais ou do processamento de categorias especiais de dados em larga escala, conforme previsão do artigo 37 da GDPR.

Tendo em vista a forte influência da GDPR na proposta regulatória brasileira, bem como o impacto internacional que esta lei geral terá a partir de sua implementação obrigatória prevista para maio de 2018, devemos estar atentos às especificidades deste marco legal em suas diferenças e similitudades com as proposições nacionais.

A fim de que possamos aproveitar as oportunidades geradas pela IoT, é vital que busquemos um ambiente regulatório favorável. Neste diapasão, conforme nos ensinam José Mauro Decoussau Machado e Pamela Gabrielle Meneguetti ao tratarem da proteção de dados na era da Internet das Coisas: "Não há dúvida que a lei está sempre um passo atrás da tecnologia, mas no caso do Brasil o atraso se verifica mesmo em relação a questões já rotineiras, o que

(127) As autoridades de controlo que não atuem como autoridade de controlo principal deverão ter competência para tratar casos a nível local quando o responsável pelo tratamento ou subcontratante estiver estabelecido em vários Estados-Membros, mas o assunto do tratamento específico disser respeito unicamente ao tratamento efetuado num só Estado-Membro, e envolver somente titulares de dados nesse Estado-Membro, por exemplo, no caso de o assunto dizer respeito ao tratamento de dados pessoais de trabalhadores num contexto específico de emprego num Estado-Membro. Nesses casos, a autoridade de controlo deverá informar imediatamente do assunto a autoridade de controlo principal. Após ter sido informada, a autoridade de controlo principal decidirá se trata o caso de acordo com o disposto em matéria de cooperação entre a autoridade de controlo principal e a outra autoridade de controlo interessada («mecanismo de balcão único»), ou se deverá ser a autoridade de controlo que a informou a tratar o caso a nível local. Ao decidir se trata o caso, a autoridade de controlo principal deverá ter em conta se há algum estabelecimento do responsável pelo tratamento ou subcontratante no Estado-Membro da autoridade de controlo que a informou, a fim de garantir a eficaz execução da decisão relativamente ao responsável pelo tratamento ou subcontratante. Quando a autoridade de controlo principal decide tratar o caso, a autoridade de controlo que a informou deverá ter a possibilidade de apresentar um projeto de decisão, que a autoridade de controlo principal deverá ter na melhor conta quando prepara o seu projeto de decisão no âmbito desse mecanismo de balcão único.

(128) As regras relativas à autoridade de controlo principal e ao mecanismo de balcão único não se deverão aplicar quando o tratamento dos dados for efetuado por autoridades públicas ou organismos privados que atuem no interesse público. Em tais casos, a única autoridade de controlo competente para exercer as competências que lhe são conferidas nos termos do presente regulamento deverá ser a autoridade de controlo do Estado-Membro em que estiver estabelecida tal autoridade pública ou organismo privado.

certamente cobra um preço alto da sociedade, seja em termos de insegurança para usuários seja por potenciais investimentos perdidos."[563]

Portanto, diante desse cenário regulatório e considerando que a regulação jurídica não deve ser vista como uma panaceia capaz de abarcar e prever todos os temas relevantes no cenário de IoT, exploraremos agora alguns complementos técnicos e conceituais de IoT. Traremos também, ao final deste capítulo, de alternativas ferramentais capazes de auxiliar o cidadão a proteger seus dados pessoais, de forma complementar à regulação jurídica.

2.5
Desafios Técnico-Regulatórios de IoT e Alternativas Ferramentais

Neste cenário de ameaça e insegurança com relação à privacidade dos usuários dentro do ecossistema de IoT, apesar das garantias existentes de proteção ao consumidor e respaldo constitucional de proteção à privacidade, sentimos falta de uma regulação específica de proteção de dados pessoais no Brasil.[564]

Pensar em uma regulação adequada para o setor é extremamente importante inclusive para que a IoT consiga cumprir seu potencial social e econômico em alinhamento com direitos fundamentais. Apesar de não termos, ainda, uma legislação específica em vigor, encontram-se em tramitação, como vimos, projetos de lei de proteção de dados pessoais inspirados pela compreensiva regulação europeia nessa área.

Porém, ainda que consigamos a aprovação de uma lei geral, enfrentamos hoje desafios adicionais técnico-regulatórios. Ainda que a legislação seja capaz de coibir abusos e trazer importantes definições conceituais com relação aos dados pessoais e seus usos, há de se considerar que, nem todos os temas estarão devidamente abarcados pela regulação e que com o avanço tecnológico da Internet das coisas, a compreensão dessa legislação torna-se cada vez mais difícil por

[563] Disponível em: <https://jota.info/artigos/protecao-de-dados-na-era-da-Internet-das-coisas-12082017#.WZGWKqFicLo.facebook>. Acesso em: 08 fev. 2017.
[564] Disponível em: <https://participacao.mj.gov.br//dadospessoais/>. Acesso em: 08 fev. 2017.

conta do tecnicismo envolvido no debate e da maior complexidade das tecnologias atuais[565].

Além disso, a regulação jurídica que recairá sobre os dados pessoais precisa de um norteamento ético mais claro debatido na esfera pública, conforme veremos no capítulo seguinte, e deve ser complementada por ferramentas (inclusive digitais) que auxiliem o cidadão a concretizar seus direitos constitucionais, conforme veremos nesse item.

Um dos desafios técnicos importantes se refere à interoperabilidade e comunicação entre os diferentes dispositivos inteligentes. Muitas das Coisas inteligentes no cenário de IoT funcionam com diferentes protocolos, podendo acarretar na impossibilidade comunicativa entre os dispositivos. No entanto, institutos de tecnologia vem desenvolvendo mecanismos para resolver este problema independente de uma regulação jurídica impondo uma uniformização de protocolos. É o caso, por exemplo do Projeto KNOT do Instituto CESAR sediado em Recife, que desenvolveu uma meta plataforma que permite a intercomunicação entre dispositivos inteligentes dotados de diferentes protocolos.[566]

Para Ramon Santos e Ronaldo Lemos, dois dos representantes do consórcio brasileiro responsável pelo Plano Nacional de IoT, o desafio está na coordenação dos órgãos reguladores e na deficiência na oferta de conexão à internet no país como um dos principais gargalos para a ampliação de uma infraestrutura conectada. Segundo os pesquisadores, não há como conectar uma determinada infraestrutura se a própria infraestrutura de conectividade não existe. Nas palavras dos autores:[567]

> Ao se tratar de infraestrutura, sobretudo a conectada, é preciso saber aonde se quer chegar, quais os objetivos e as metas, como coordenar os esforços entre governo federal, Estados e municípios, bem como a maneira de implementar e fiscalizar as ações necessárias para executar o projeto.
> (...)
> Com a previsão de conexão de milhares dispositivos às redes de telecomunicações do país e o consequente crescimento exponencial do tráfego de dados é fundamental criar modelos de expansão da internet para permitir investimentos, abrindo caminho para viabilizar esse modelo.

[565] ZIEGELDORF, Jan, MORCHON, Oscar e WHERLE Klaus. "*Privacy in the Internet of Things: Threats and Challenges*". Security and Communications. Volume 7, issue 12, 2014. pp.2728-2742.
[566] Disponível em: <https://www.knot.cesar.org.br/>. Acesso em: 08 fev. 2017.
[567] Disponível em: <http://m.folha.uol.com.br/mercado/2017/12/1944851-planejamento-e-essencial-para-conectar-infraestrutura.shtml>. Acesso em: 08 fev. 2017.

> (...)
> Planejamento de médio e de longo prazo não costuma ser o forte do país. Nem a coordenação de esforços entre os entes federativos. Esse talvez seja o maior obstáculo para o Brasil fazer decolar sua infraestrutura conectada.

É importante termos em mente que sempre que falamos em infraestrutura conectada, estamos falando de questões regulatórias. Nesse sentido, o primeiro passo deve ser a aprovação de uma lei que trate da proteção aos dados pessoais. Os desafios técnicos levantados nesse capítulo são importantes para chegarmos a uma regulação eficiente e adequada ao cenário de IoT.

Rolf H. Weber, em seu artigo *"Internet of Things- New security and privacy challenges"* [568] argumenta que uma legislação a nível internacional combinada com um modelo de "*self-regulation"* seria a alternativa mais benéfica por conta da perspectiva de implementação global que a IoT terá. O autor ressalta, contudo, que a abordagem do "*self-regulation*" poderia ser perversa, caso não viesse acompanhada de um marco regulatório básico. Isso ocorreria por que a pressão dos membros do mercado pode não ser o suficiente para obrigar determinadas empresas a terem o mesmo padrão de conduta. Nesse sentido, o autor sugere a criação de um marco regulatório para a questões de privacidade e segurança a nível internacional.

Como os interesses sobre essas questões não são os mesmos em todos os países, Weber argumenta que o legislador somente criaria o conjunto de regras básico voltado ao plano internacional, sendo os detalhes a serem complementados pelo setor privado. O papel do Estados, nesse cenário, se resumiria a ser um co-regulador, fiscalizando se o setor privado está a cumprir as diretrizes básicas fixadas no plano internacional, bem como, os parâmetros fixados internamente.[569]

Scott Peppet, por outro lado, argumenta por um mecanismo de regulamentação capitaneado pelo próprio Estado e pelos cidadãos. Ele define quatro passos que devem ser tomados para se ter uma proteção aos dados dos usuários desses produtos de forma eficiente: [570]

---

[568] WEBER, Rolf H. *Internet of Things:* New Security and Privacy Challenges, Computer Law 8L Security Report, January 2010.
[569] WEBER, Rolf. Internet of Things- New security and privacy challenges. Computer Law & Security Review; 2010. pp. 23-30.
[570] PEPPET, Scott R. Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent. Texas Law Review. Volume 93, 2015.pp 148.

> (i) Ampliar as políticas nacionais relacionadas a proteção de dados pessoais, com o intuito de dissuadir as possibilidades de discriminação oriunda do acesso a esses dados.
> (ii) Redefinir o significado de "personally identifiable information" (PII), de modo a englobar dados oriundos de objetos IoT, como a biometria.
> (iii) Expansão da aplicação das notificações estaduais, com o intuito de elas abarcarem as violações de privacidade e segurança na Internet das coisas.
> (iv) Aumentar as possibilidades de um consentimento às políticas de dados de forma consciente por meio do acompanhamento de como as notificações e as escolhas dos usuários devem ser explicitadas em objetos de tecnologia IoT. [571]

A opção por uma regulamentação estatal também parece ser a opinião de Bruce Schneier, criptógrafo e especialista em segurança computacional, em uma recente audiência pública realizada pelo Congresso americano, Bruce argumenta que[572]:[573]

> O comprador e o vendedor não se importam. Além disso, o Sr. Burgess apontou para este fato. O comprador e o vendedor querem um dispositivo que funcione. Esta é uma externalidade econômica. Eles não sabem sobre isso e não faz parte da decisão. Então eu argumento que o governo tem que se envolver, que isso é uma falha de mercado, e o que eu preciso são alguns bons regulamentos.[574]

Nessa mesma audiência, Kevin Fu, membro do departamento de engenharia elétrica e ciência da computação da universidade de Michigan, afirma acreditar que o governo deve efetuar medidas com o intuito de criar um espaço de IoT minimamente seguro. O primeiro seria por meio do incentivo às empresas que produzem objetos com essa tecnologia realizarem a *"cybersecurity hygiene"*, a qual se consubstancia, por exemplo, na criação de sistemas com criptografias eficientes. O segundo seria o incentivo às instituições de pesquisa e ensino superior desse ramo para que a formação de profissionais de cyber-segurança seja robusta. O terceiro seria analisar a viabilidade de criação de uma instalação, nacional e independente, destinada a testar a segurança dos objetos de IoT. O quarto seria realizar o incremento de conhecimento sobre cyber segurança às agências especializadas no setor de tecnologia. Por fim, Fu argumenta que o

[571] PEPPET, Scott R. Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent. Texas Law Review. Volume 93, 2015.pp 148.
[572] Audiência pública "*Understanding the role of connected in recent cyber attacks"* realizada no dia 16 de novembro de 2016. Disponível em: https://www.youtube.com/watch?v=BvId5-0295U Acesso em: 14/02/2017
[573] Tradução livre do autor. No original: *The buyer and seller don't care. In addition, Mr. Burgess pointed this out. The buyer and seller want a device that works. This is an economic externality. They don't know about it and it is not part of the decision. So I argue that government has to get involved, that this is a market failure, and what I need are some good regulations.*
[574] Idem.

somatório das iniciativas do governo, universidades e o setor privado seria o ideal para alterar a atual infraestrutura no setor de IoT. [575]

Debasis Bandyopadhyay e Jaydip Sen, em seu texto *"Internet of Things: Applications and Challenges in Technology and Standardization"*[576], argumentam que a expansão no cenário de IoT demanda, ainda, uma troca do Sistema de RFID para o Sistema de UID (*unique/universal/ubiquitous identifier*). Essa é a proposta, inclusive, do consórcio *CASAGRAS.* No cenário regulatório brasileiro, contudo, a possível alteração desse sistema traria desafios sob quais conjuntos de regras se tornariam aplicáveis.

Os autores explicitam que na perspectiva desse consórcio:[577]

> Nesta perspectiva, a IoT torna-se a arquitetura habilitadora natural para a implantação de serviços e aplicativos federados independentes, caracterizados por um alto grau de captura autônoma de dados, transferência de eventos, conectividade de rede e uma interoperabilidade.

Todavia, compreendendo esse como um cenário já presente, precisamos de regras para a coleta e análise de dados que já trafegam, protegendo a privacidade de cidadãos e usuários. Segundo opinião dos representantes do consórcio do Plano Nacional de IoT, implementar infraestrutura conectada sem uma lei desse tipo traz sérios riscos a direitos fundamentais. Portanto, "privacidade de dados e infraestrutura conectada são dois lados da mesma moeda".[578]

Veremos, no item seguinte, algumas respostas técnicas e teóricas ao cenário de falta de regulamentação e tutela adequada da privacidade e dos dados pessoais, para fins de coibir abusos e melhor garantir os direitos constitucionais dos cidadãos.

---

[575] Idem.

[576] Debasis Bandyopadhyay e Jaydip Sem. "Internet of Things: Applications and Challenges in Technology and Standardization". Wireless Personal Communications, Volume 58, issue 1, pp.49-69., 2011.

[577] Tradução livre do autor. No original: *From this perspective, IoT becomes the natural enabling architecture for the deployment of independent federated services and applications, characterized by a high degree of autonomous data capture, event transfer, network connectivity and an interoperability.*

[578] Disponível em: <http://m.folha.uol.com.br/mercado/2017/12/1944851-planejamento-e-essencial-para-conectar-infraestrutura.shtml>. Acesso em: 08 fev. 2017.

2.5.1
A Internet das Coisas Anônimas e o Direito ao Não-Rastreio

Em uma sociedade hiperconectada a privacidade deve ser compreendida de maneira funcional, propiciando ao indivíduo a possibilidade deste conhecer, controlar, endereçar e interromper o fluxo das informações a ele relacionadas[579]. Esse direito está intrinsecamente relacionado à salvaguarda da dignidade e da personalidade do indivíduo, consubstanciada nas determinações constitucionais e infraconstitucionais referentes à vida privada, intimidade e inviolabilidade de dados[580].

No contexto de IoT, a ausência de uma regulação jurídica suficiente para tutelar o cidadão, juntamente com as frequentes abusividades referentes ao armazenamento, tratamento e monetização de dados pessoais, eleva a preocupação com a proteção da privacidade a um novo patamar.

Muitas pessoas, conscientes deste cenário, buscam por ferramentas de anonimização *online* e acessos globais à Internet por meio de redes como o TOR (*The Onion Router*)[581] que vêm crescendo nos últimos anos. TOR consiste em um acrônimo para *The Onion Router*, se tratando de um software livre que proporciona o anonimato pessoal ao navegar na Internet e em atividades online, protegendo contra a censura e principalmente a privacidade pessoal. Esse tipo de ferramenta proporciona o anonimato pessoal ao navegar na Internet e em atividades online, protegendo contra a censura e principalmente a privacidade pessoal.

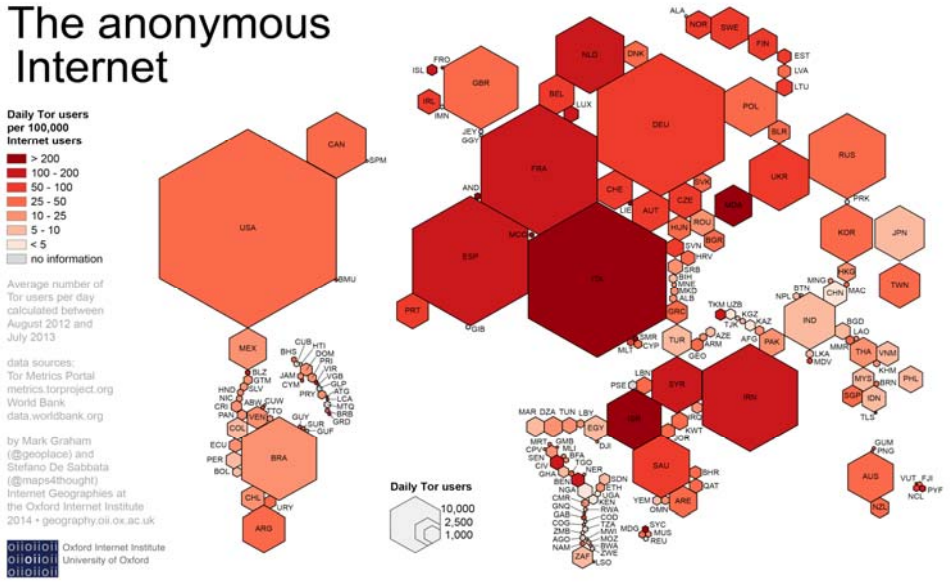
---

[579] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 92-95.

[580] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*. São Paulo: Editora Revista dos Tribunais, 2012, p. 390.

[581] "O anonimato só poderá ser garantido se o usuário puder remover ou impedir a exposição dos seus rastros online. As comunicações na Internet baseiam-se em uma linguagem de comunicação (denominado de "protocolo"), que atribui para cada computador conectado um número que serve de endereço para o envio de informações, e que também identifica esse computador. É o chamado número IP, composto de uma série de 4 grupos, e que, para os computadores comuns, é modificado a cada conexão. Logo, para identificar um computador, não basta o seu IP, é preciso também o dia e hora dessa comunicação. Se o IP identifica o computador, um usuário, para garantir o seu anonimato, precisa ocultar o número, por processos como a rede virtual privada (VPN – Virtual Privacy Network), ou, dentre outras técnicas pelo uso de um número IP de terceiros, o que pode ser realizado através de programas como o TOR – The Onion Network38 ou pela utilização de redes de terceiros". CAPANEMA, Walter. O direito ao anonimato: uma nova interpretação do art. 5o, IV, CF.

A imagem reproduzida a seguir consiste em um mapa cartográfico elaborado por pesquisadores do Oxford Internet Institute.[582]Eles se basearam em informações disponíveis no portal Tor Metrics[583], o qual nos auxilia a observar a dinâmica dos acessos globais[584] à Internet através de redes TOR[585].



(Link para mapa: http://geography.oii.ox.ac.uk/?page=tor).

Entretanto, esse movimento ainda suscita polêmicas éticas, legais e técnicas. Diversos doutrinários e profissionais do setor privado vêem no anonimato *online* uma grande saída para "terroristas em potencial" [586] que objetivam ofender, difamar, caluniar[587], dentre outros. No setor público, o governo caminha no sentido de criminalizar a anonimização *online*, acreditando inclusive que, nesses casos, cabe às instituições governamentais rastrear dispositivos que instalem tais sistemas[588].

Em sentido oposto às críticas acadêmicas, morais, técnicas e governamentais ao anonimato *online*, Glenn Greenwald[589] e Julian Assange[590],

[582] Disponível em: <https://www.oii.ox.ac.uk/>. Acesso em: 20 nov. 2017.
[583] Disponível em: <https://metrics.torproject.org/>. Acesso em: 20 nov. 2017.
[584] Disponível em: <https://www.oii.ox.ac.uk/>. Acesso em: 20 nov. 2017.
[585] Acrônimo para The Onion Router é um software livre que proporciona o anonimato pessoal ao navegar na Internet e em atividades online.
[586] SCHMIDT, Eric; COHEN, Jared. *The new digital age: Reshaping the future of people, nations and business*. Londres: Hachette UK, 2013.
[587] BAUMAN, Zygmunt. Sobre a internet, anonimato e irresponsabilidade In: *Isto não é um diário*. Rio de Janeiro: Zahar, 2012.
[588] Vide "Rule 41" das Federal Rules of Criminal Procedure, U.S. Supreme Court.
[589] GREENWALD, Glenn. Sem lugar para se esconder. Rio de Janeiro: Sextante, 2014, p. 263.

defendem a viabilização de "formas específicas de tecnologia que garantam direitos e liberdades fundamentais" - como liberdade de expressão e privacidade - por meio da possibilidade de anonimato no cenário de hiperconectividade. Segundo o jornalista e ativista Glenn Greenwald: "para impedir os governos de se intrometerem em suas comunicações e em sua atividade pessoal na internet, todos os usuários deveriam adotar ferramentas de criptografia e de anonimato para a navegação.

Essa postura converge com um valor fortemente associado à cultura *hacker*[591], a saber, a *expertise* tecnológica pode contribuir para equilibrar as relações de poder na sociedade, permitindo que os cidadãos resistam contra as diversas ameaças de invasão de privacidade na era digital. Nessa perspectiva, a democratização e a disseminação de práticas de anonimização *online* constituem métodos não violentos de proteção da privacidade (ou "*hacking* defensivo").[592]

Na esteira do que vem se explicando, cabe trazer à tona a discussão teórica acerca da abordagem eminentemente etimológica para a concepção de "anonimato". Apesar de a definição primária do mencionado termo compreender a noção de algo ou alguém inominado, quando tratamos de um contexto conectado esta passa a não dizer respeito ao "nome", seja ele real ou fictício, mas a quaisquer mecanismos de identificação pessoal[593].

Nos ajudam a assimilar essa tese Marx e Nissenbaum, ao mostrarem, respectivamente, que: i) ainda que *off-lines* podemos ser identificados por meio de informações como localização física ou lógica (endereço ou CEP), padrão de conhecimento (aparência ou comportamento), categorização social (gênero, ideologia, orientação sexual etc.), dentre outros[594]; e ii) tecnologias de rastreio

---

[590] ASSANGE, Julian et al. *Cypherpunks: Liberdade e o future da Internet*. São Paulo: Boitempo, 2013.

[591] Para detalhes acerca da "cultura hacker", inclusive sua heterogeneidade e diversidade de valores, ver: Pekka Himanen, *The Hacker Ethics – and the Spirit of Information Age*. NY: Random House Trade Paperbacks, 2001; Tim Jordan*, Activism! Direct Action, Hactivism and the Future of Society*. London: Reaktion Books, 2002; Douglas Thomas, *Hacker Culture*: Minneapolis/London: University of Minnesota Press, 2003; Jon Erickson, *Hacking – the art of exploitation*. San Francisco: No Starch Press, 2008; Steven Levy, *Hackers*. Sebastopol: O'Relly, 2010; Gabriella Coleman, *Coding Freedom – The ethics and aesthetics of hacking*. Princeton: Princeton University Press, 2012.

[592] ASSANGE, Julian et al. *Cypherpunks: Liberdade e o future da Internet*. São Paulo: Boitempo, 2013.

[593] LIDDELL and SCOTT. *Greek-english Lexicon*. 7. ed. Nova Iorque: Oxford, 2001.

[594] G. Marx, "*What's in a Name?* Some Reflections on the Sociology of Anonymity", The Information Society 15(2):99-112 · May 1999

digital podem rastrear indivíduos, mesmo que inominados, por meio de estatísticas analíticas por extração de dados (*data mining*), *click-stream tracking* (rastreio de interesses), coleta automática de dados (*downloads*, IP e histórico de navegação), entre outras coisas [595]. No cenário de IoT, a capacidade de monitoramento, rastreio e identificação abusiva do consumidor se insere em um novo patamar de risco por conta dos inúmeros dispositivos conectados processando dados.

Desta forma, chega-se à conclusão de que atualmente a identificação pessoal deixou de decorrer da mera identificação do "nome" e passou a se relacionar com a possibilidade técnica de rastreio de dados agregados a objetos conectados à rede internacional de computadores. Com isso em mente, Kathleen Wallace[596] concebeu um conceito singular de anonimato *online*, centralizado na noção de "não coordenação de traços conhecidos" (características, ações, endereços etc.) em dadas relações comunicativas.

Nesta perspectiva, defende-se neste trabalho que o conceito de privacidade deve ser ampliado em comparação à sua significação original ("direito de ser deixado só" ou *right to be let alone*)[597]. O conceito de privacidade e proteção de dados pessoais na era da hiperconectidade relacionada à IoT deve englobar um *direito ao não-rastreio (Right to non-tracking)*[598]. Neste diapasão, as ferramentas de anonimato *online* devem ser retratadas como uma *resistência ao rastreio digital* nos casos em que sirvam para a concretização legítima e proporcional de direitos fundamentais.

O conceito transcende, assim, tanto o caráter de liberdade negativa (liberdade de não ser impedido ou de não ser obrigado a fazer algo)[599] como o de

[595] NISSENBAUM, Helen. *The Meaning of Anonymity in an Information Age*. The Information Society, 15:141-144, 1999.
[596] Wallace, K.A. (1999) *Anonymity.* Ethics and Information Technology 1 (1), 23-35. Wallace, K.A. (2008) On-line Anonymity. Entry for Handbook on Information and Computer Ethics, eds. Herman Tavani and Ken Himma, John Wiley & Sons, Inc., 165-189.
[597] WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy.* Harvard Law Review, v. 4, n. 5, 1890, p. 193-220.
[598] Essa tese foi levantada em artigo anterior do autor deste trabalho, na revista Internet Policy Review em 2017. Disponível em: <https://policyreview.info/articles/news/emergence-internet-anonymous-things-aniot/693. https://policyreview.info/tags/right-non-tracking>. Acesso em: 20 nov. 2017.
[599] Como conceitua Norberto Bobbio, "[p]or liberdade negativa, na linguagem política, entende-se a situação na qual um sujeito tem a possibilidade de agir sem ser impedido, ou de não agir sem ser obrigado, por outros sujeitos. (...) A liberdade negativa costuma também ser chamada de liberdade como ausência de impedimento ou de constrangimento: se, por impedir, entende-se não permitir

liberdade positiva[600] (liberdade como autonomia, liberdade enquanto possibilidade de direcionar seu próprio querer sem ser determinado por outros, ligada ao controle dos dados, o que se deve ao contexto social advindo de evoluções tecnológicas.).[601] Com efeito, a noção de privacidade na era da informação também deve englobar o próprio controle dos dados digitais.[602] Compreende, portanto, capacidades cognitivas e materiais para formular e investir voluntariamente, pelo maior tempo e extensão possíveis, instrumentos tecnológicos (como navegadores, buscadores, aplicativos, *softwares*, dentre outros) e conhecimentos técnicos visando garantir a invisibilização de informações e dados particulares mediante o controle da interceptação, coleta, análise, monitoramento, armazenamento ou rastreio digital de metadados confidenciais ou de dispositivos privativos conectados à rede mundial de computadores.[603]

Entretanto, no momento em que o cenário peculiar da IoT é considerado, o debate genérico alusivo à privacidade *online* - especialmente aquela tocante ao anonimato - alcança um outro patamar, visto que nesse caso questões como "será

---

que outros façam algo, e se, por constranger, entende-se que outros sejam obrigados a fazer algo, então ambas as expressões são parciais, já que a situação de liberdade chamada de liberdade negativa compreende tanto a ausência de impedimento, ou seja, a possibilidade de fazer, quanto a ausência de constrangimento, ou seja, a possibilidade de não fazer." (BOBBIO, Norberto. Igualdade e liberdade. Tradução: Carlos Nelson Coutinho. 2. ed. Rio de Janeiro: Ediouro, 1997, p. 48-49).

[600] Para Bobbio, [p]or liberdade positiva, entende-se -na linguagem política -a situação na qual um sujeito tem a possibilidade de orientar seu próprio querer no sentido de uma finalidade, de tomar decisões, sem ser determinado pelo querer de outros. Essa forma de liberdade é também chamada de autodeterminação ou, ainda mais propriamente, de autonomia" (BOBBIO, Norberto. Igualdade e liberdade. Tradução: Carlos Nelson Coutinho. 2. ed. Rio de Janeiro: Ediouro, 1997, p. 51).

[601] Sobre o tratamento da privacidade como liberdade negativa ou positiva, v. MACEDO JÚNIOR, Ronaldo Porto. Privacidade, Mercado e Informação. *Justitia,* São Paulo, n. 61, jan./dez. 1999, p. 245-259.

[602] Caitlin Mulholland, por exemplo, apresenta três concepções sobre o direito à privacidade, quais sejam, "(i) o direito de ser deixado só, (ii) o direito de ter controle sobre a circulação dos dados pessoais, e (iii) o direito à liberdade das escolhas pessoais de caráter existencial" e acrescenta a esta lista o direito de não tomar conhecimento acerca de um dado pessoal". (MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. *Civilistica.com*, Rio de Janeiro, v. 1, n. 1, p. 3, 2012).

[603] Alguns traços relevantes da anonimização *online* perpassam pela ideia de gradualidade (distribui-se por níveis: fraco/forte, mínimo/máximo), circunstancialidades (depende de ferramentas e saberes), volitividade (envolve uma intenção de anonimização), parcialidade (não total), contextualidade (refere-se a traços específicos), e bidirecionalidade (relação de pessoa/dispositivo A com B). Cole Stryker. *Hacking the Future. Privacy, Identity, and Anonymity on the Web.* NY: Overlook Duckworth, 2012.

possível garantir ao mesmo tempo uma hiperconectividade e proteger a privacidade? O que seria uma "coisa" anônima na IoT?[604], ganham destaque.

Neste sentido, Roman, Najera & Lopez[605] relacionam alguns obstáculos para a implementação cabal da IoT no que tange à privacidade e segurança, como o risco de ataques (DDoS; clonagem/emulação de RFID; *cracking*), erros no funcionamento (*spamming*), insuficiência das proteções digitais usuais (protocolos de segurança; garantias de privacidade; métodos criptográficos) e a estrutura técnica e legal. No mesmo caminho segue Miorandi et. al[606] ao sustentar que a segurança é um "componente crítico" para a adesão integral das tecnologias e aplicações da IoT, repisando ainda a insuficiência de soluções não *ad hoc* de confidencialidade, autenticidade e privacidade.

Ziegeldorf, Morchon & Wehrle [607], por outro lado, entendem a interconexão e extensa comunicação de dispositivos inteligentes como uma "evolução da internet" rumo ao "mundo real". Porém, admitem que a "coleta ou rastreio de dados ubíquos" representa um risco para a privacidade, que traz incertezas em relação ao sucesso cabal da IoT.

Jing et al.[608] destacam que as ameaças à segurança e privacidade no cenário da IoT conta com similaridades com aquelas das redes tradicionais, mas reconhece que a IoT apresenta um "ambiente mais perigoso". Deste modo, sugerem um tipo de proteção da arquitetura do sistema que compreenda pelo menos três camadas mínimas: (i) Camada de percepção (*Uniform Coding, Conflict Collision, RFID Privacy Protection, Trust Management*); (ii) Camada de transporte (*network access control technology*); e (iii) Camada de aplicação (*network control technology, communications technology* e *mobile terminal technology*).

---

[604] Sobre desta proposta de reflexão, v. CASTRO, Marco Aurélio. *Direito e pós-humanidade: quando os robôs serão sujeitos de direito*. Curitiba: Juruá. 2013.
[605] ROMAN, Rodrigo, NAJERA, Pablo e LOPEZ, Javier. Securing the Internet of Things. *IEEE Computer*, vol. 44, 2011, p. 51-58.
[606] MIORANDI, Daniele et al. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, vol. 10, 2012, p. 1497-1516.
[607] ZIEGELDORF, Jan, MORCHON, Oscar e WEHRLE, Klaus. Privacy in the Internet of Things: threats and challenges. *Security Comm*. Networks, vol. 7, n. 12, 2014.
[608] JING, Qi et. al. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, v. 20, n. 8, 2014, p. 2481-2501.

Sicari et al.[609], finalmente, retratam a IoT como um aglomerado de tecnologias heterogêneas que contam com serviços inovadores que trazem à tona tópicos relacionados às "exigências de privacidade" e à "satisfação com segurança", dentre os quais se incluem a confidencialidade de dados, controle de acesso à rede, autenticação, políticas de segurança e privacidade e confiança entre usuários. Nesse contexto, pode-se afirmar que esses tópicos apontam no sentido da deficiência dos métodos tradicionais face aos padrões flexíveis e infraestrutura da IoT.

Como se pode perceber, há uma discussão crescente e diversificada sobre privacidade e segurança na atual bibliografia especializada sobre o tema: (i) em *livros*: Michahelles[610], Wang & Zhang[611], Boswarthick & Elloumi[612], McEwen & Cassimally[613], Nik Bessis & Ciprian Dobre[614], Jan Höller[615], Joe Weinman & Fred Wiersema[616], Jonathan Follett[617], Nitesh Dhanjani[618] ou Philip N. Howard[619]; (ii) em *manuais técnicos*: Daniel Kellmereit & Daniel Obodovski[620], Shancang Li et. al.[621], Salvatore Gaglio & Giuseppe Lo Re[622], Hazim Dahir, Bil Dry & Carlos

[609] SICARI, S. et al. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, v. 76, 2015, p. 146-164.
[610] UCKELMANN, Dieter; HARRISON, Mark; MICHAHELLES, Florian. *Architecting the internet of things*. Berlim: Springer, 2011.
[611] WANG, Yongheng; ZHANG, Xiaoming (Ed.). *Internet of Things:* International Workshop, IOT 2012, Changsha, China, August 17-19, 2012. Nova York: Springer, 2012.
[612] HERSENT, Olivier; BOSWARTHICK, David; ELLOUMI, Omar. *The internet of things:* Key applications and protocols. Hoboken: John Wiley & Sons, 2011.
[613] MCEWEN, Adrian; CASSIMALLY, Hakim. *Designing the internet of things*. Hoboken: John Wiley & Sons, 2013.
[614] BESSIS, Nik e DOBRE, Ciprian. *Big Data and internet of things:* a roadmap for smart environments. Nova York: Springer International Publishing, 2014.
[615] HOLLER, Jan et al. *From Machine-to-machine to the Internet of Things:* Introduction to a New Age of Intelligence. Cambridge: Academic Press, 2014.
[616] WEINMAN, Joe. *Digital Disciplines:* Attaining Market Leadership via the Cloud, Big Data, Mobility, Social Media, and the Internet of Everything. Hoboken: John Wiley & Sons, 2015.
[617] FOLLETT, Jonathan. *Designing for Emerging Technologies:* UX for Genomics, Robotics, and the Internet of Things. Newton: O'Reilly Media, Inc., 2014.
[618] DHANJANI, Nitesh. *Abusing the Internet of Things:* Blackouts, Freakouts, and Stakeouts. Newton: O'Reilly Media, Inc., 2015.
[619] HOWARD, Philip N. *Pax Technica:* How the Internet of things may set us free or lock us up. New Haven: Yale University Press, 2015.
[620] KELLMEREIT, Daniel e OBODOVSKI, Daniel. *The Silent Intelligence:* the internet of things. São Francisco: DnD Ventures, 2013.
[621] LI, Shancang; XU, Li. *Securing the Internet of Things*. Cambridge: Syngress, 2017.
[622] GAGLIO, Salvatore; RE, Giuseppe Lo. *Advances onto the Internet of Things*. Nova York: Springer, 2014.

Pignataro[623], Othmar Kyas[624], Peter Waher[625], Robert Stackowiak et al.[626] ou Alasdair Gilchrist[627]; e (iii) em *artigos*: Atzori et al.[628], Bandyopadhyay & Sem[629], Roman, Najera & Lopez[630], Tobias Heer et al.[631], Miorandi et al.[632], Bin Guo et al.[633], Roman et al.[634], Ziegeldorf et al.[635], Chabridon et al.[636], Qi Jing et al.[637], Borgia[638], Ashraf et al.[639] ou Sicari et al.[640]. No entanto, esse desenvolvimento se contrapõe ao limitado espaço destinado à inexplorada questão do anonimato *online* no contexto da IoT.

De modo esquemático, o debate sobre anonimato *online* na IoT (AnIoT) pode ser subdividido nos seguintes grupos analíticos: (1) Gerenciamento de identidade dos objetos; (2) Mecanismos de proteção da privacidade; (3) Proteção

[623] DAHIR, Hazim, DRY, Bil e PIGNATARO Carlos. *People, Processes, Services, and Things:* Using Services Innovation to Enable the Internet of Everything. Nova York: Business Expert Press, 2015.
[624] KYAS, Othmar. *How To Smart Home:* A Step by Step Guide to Your Personal Internet of Things. Wyk auf Föhr (Alemanha): Key Concept Press, 2015.
[625] WAHER, Peter. *Learning internet of things*. Birmingham: Packt Publishing Ltd, 2015.
[626] STACKOWIAK, Robert et al. Big Data and the Internet of Things: Enterprise Information Architecture for a New Age. Nova York: Apress, 2015.
[627] GILCHRIST, Alasdair. Introducing Industry 4.0. In: *Industry 4.0.* Nova York: Apress, 2016. p. 195-215.
[628] ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. *Computer networks*, v. 54, n. 15, 2010, p. 2787-2805.
[629] BANDYOPADHYAY, Debasis; SEN, Jaydip. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, v. 58, n. 1, 2011, p. 49-69.
[630] ROMAN, Rodrigo, NAJERA, Pablo e LOPEZ, Javier. Securing the Internet of Things. *IEEE Computer*, vol. 44, 2011, p. 51-58.
[631] HEER, Tobias et al. Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, v. 61, n. 3, p. 527-542, 2011.
[632] MIORANDI, Daniele et al. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, vol. 10, 2012, p. 1497-1516.
[633] GUO, Bin et al. From the internet of things to embedded intelligence. *World Wide Web*, v. 16, n. 4 2013, p. 399-420.
[634] ROMAN, Rodrigo; ZHOU, Jianying; LOPEZ, Javier. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, v. 57, n. 10, p. 2266-2279, 2013.
[635] ZIEGELDORF, Jan, MORCHON, Oscar e WEHRLE, Klaus. Privacy in the Internet of Things: threats and challenges. *Security Comm*. Networks, vol. 7, n. 12, 2014.
[636] CHABRIDON, Sophie et al. A survey on addressing privacy together with quality of context for context management in the internet of things. *Annals of telecommunications-annales des télécommunications*, v. 69, n. 1-2, 2014, p. 47-62.
[637] JING, Qi et al. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, v. 20, n. 8, 2014, p. 2481-2501.
[638] BORGIA, Eleonora. The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, v. 54, 2014, p. 1-31.
[639] ASHRAF, Qazi Mamoon; HABAEBI, Mohamed Hadi. Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, v. 49, 2015, p. 112-127.
[640] SICARI, Sabrina et al. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, v. 76, 2015, p. 146-164.

contra a associação de "biodado" à identidade/endereço IP; (4) Proteção da privacidade em tecnologias RFID de esquemas baseados em senhas e; (5) Impedir usuários (humanos e máquinas) não autorizados de acessar o sistema.

Uma forma de aprimorar a discussão em comento pode estar relacionada às pesquisas sobre *Privacy Enhancing Technologies*[641]. Em linhas gerais, existem pesquisas em desenvolvimento sobre temas específicos como: (i) à P3P – *Platform for Privacy Preferences* (por exemplo, a programação do próprio *browser*), (ii) iniciativas de certificação digital referentes a técnicas, práticas e procedimentos em infraestrutura de chave pública (ICP), e (iii) ao nível indivíduo/objeto/transação/dado e sistema. No domínio técnico, sobressaem o recurso a VPNs (*Virtual Private Networks*), TLS (*Transport Layer Security*), DNS Security Extensions, Roteamento por camadas, PIR (*Private Information Retrieval*), Sistemas *peer-to-peer* (P2P) ou RFID Tags. Todavia, é crucial ter em mente, neste momento, que todas as abordagens destacadas possuem vantagens e desvantagens[642].

A premência da IoT insere o debate sobre segurança e privacidade em um novo contexto. Nesse sentido se posicionam Weber e Weber[643], indicando que somente uma abordagem global da privacidade, isto é, que compreenda os aspectos supracitados[644], propiciará uma navegação segura na IoT. Nesta conjuntura, é fundamental a concepção de abordagens regulatórias, educativas e técnicas para tratar dos potenciais riscos à privacidade, falhas na confidencialidade, autoproteção através da anonimização), interação segura e identificação e notificação de falhas.

Os tópicos relacionados a segurança e privacidade são cruciais para que a IoT possa ser plenamente implementada. Nesse sentido, reconhece-se a importância de soluções sólidas para assuntos como autenticidade, confidencialidade e privacidade, perpassando ainda por modelos e padrões

[641] FISCHER-HÜBNER, Simone; WRIGHT, Matthew (Ed.). Privacy Enhancing Technologies: 12th International Symposium, PETS 2012, Vigo, Spain, July 11-13, 2012, *Proceedings*. Nova York: Springer, 2012.
[642] WEBER, Rolf H.; WEBER, Romana. *Internet of things*. Nova York: Springer, 2010.
[643] Ibid.
[644] Para uma introdução ao debate sobre educação tecnológica e anonimização, ver BAGGIO, Bobbe; BELDARRAIN, Yoany. *Anonymity and Learning in Digitally Mediated Communications:* Authenticity and Trust in Cyber Education. IGI Global, 2011.

inovadores de tutela da arquitetura do sistema que abranjam as camadas de percepção, transporte e aplicação.

Não obstante, ainda que tenha havido um aumento significativo nas discussões sobre segurança e privacidade no cenário da IoT, há uma escassez de artigos, livros ou mesmo manuais técnicos que abordem o tema do anonimato *online* neste cenário.

Como se pôde notar, a IoT eclode como um dos contextos contemporâneos mais desafiadores no que tange à proteção da privacidade e dos dados pessoais. Seu potencial de coleta, transmissão, armazenamento e compartilhamento de dados pessoais/sensíveis de indústrias, empresas, equipamentos, indivíduos e instituições gera grandes provocações ético-legais, considerando a infindável conexão comunicativa entre pessoas-máquinas e máquinas-máquinas através de redes sem fio. A era da informação acarretou a criação de variadas tecnologias de rastreio de dados pessoais e sensíveis relacionados a dispositivos conectados à Internet. Por conta disso, a noção tradicional de privacidade enquanto "direito de ser deixado só" (*right to be let alone*) se mostra insuficiente frente ao contexto de hiperconectividade criado pela IoT.

Deste modo, é importante que haja uma modificação conceitual acerca da concepção de privacidade, de forma que essa compreenda a noção de "não rastreio" (ou da "não coordenação de traços conhecidos" como características, ações, endereços etc.) em certas interações comunicativas. O argumento do anonimato *online* vinculado a um *direito ao não-rastreio* (e, consequentemente, não-coleta, não-transmissão, não-armazenamento e não-compartilhamento) traz, de fato, um arcabouço mais adequado a respeito da adequação da privacidade e da proteção dos dados digitais.

Conquanto o anonimato seja compreendido muitas vezes como proibido em função de uma leitura literal do art. 5º inc. IV da Constituição Federal, merece ter sua legitimidade (*on-line* e *off-line*) melhor assimilada e prestigiada em situações nas quais constitui ferramenta essencial para a preservação de direitos constitucionais (não somente relacionado à liberdade de expressão, mas também ao acesso à informação e ao direito à privacidade).[645]

[645] MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.

Devemos levar em consideração que a Constituição Federal não foi pensada para a era da hiperconectividade e da IoT em que o tratamento dos dados pode gerar uma série de abusos e prejuízos pessoais e coletivos.

O uso instrumental do anonimato não serve somente para o cometimento de ilícitos. A reinterpretacao judicial deve encarar o anonimato em determinadas circunstâncias como uma ferramenta que permite à Constituição acompanhar a evolução social e preservar os demais valores fundamentais.[646] Em alternativa, quando o anonimato (seja este *online* ou não) for utilizado como instrumento para o cometimento de ilícitos de qualquer natureza, deve ser visto como ilegítimo.[647]

Nas palavras de Walter Capanema:[648]

> Muito embora a literalidade do art.5o, IV da Constituição Federal proíba o anonimato, tendo em vista a importância que esse instituto é para a salvaguarda da identidade, vida, liberdade e honra do indivíduo, propõe-se uma reinterpretação dessa norma em consonância com a própria liberdade de expressão, de modo a afirmar que o anonimato vedado pela Carta Magna é só aquele que cause prejuízos a terceiros. O anonimato, sem dúvida alguma é um escudo contra a tirania, de onde quer que ela surja.

Portanto, é imprescindível o avanço de uma análise técnica e jurídica relacionada ao ajuste da tese do direito ao não-rastreio[649] ao cenário da IoT. A noção de uma Internet das Coisas Anônimas enquanto instância da privacidade e da proteção dos dados pessoais na IoT ainda precisa de maiores esclarecimentos conceituais e análises de viabilidade técnica, dado que, como anteriormente

---

[646] Primeiramente, é um equívoco considerar que o anonimato é completamente vedado no Brasil. Isso porque o art. 5º inc. IV se refere especificamente a "manifestação do pensamento", portanto não pode ser estendida essa limitação para outros casos. Ainda assim, mesmo especificamente com relação à manifestação do pensamento, há quatro motivos para embasar a reinterpretação do dispositivo (ainda que seja cláusula pétrea) permitindo o anonimato: (i) por não gerar prejuízos a terceiros; (ii) por ampliar e concretizar melhor outros direitos fundamentais como privacidade, acesso à informação e liberdade de expressão, tendo em vista que a Constituição Federal de 1988 não foi pensada para a era da hiperconectividade e da IoT; (iii) por representar um perigo democrático maior abrir uma constituinte e; (iv) por já haver precedentes de reinterpretação deste dispositivo como a legitimidade da denúncia anônima no Brasil. Com relação especificamente ao ambiente online, regulado no Brasil infra-constitucionalmente, o Marco Civil da Internet garante o sigilo nas comunicações realizadas através da Internet, desde que o usuário possa ser 'identificável' (portanto o acesso somente aos meta-dados já seria suficiente), não necessitando estar expressamente identificado nas comunicações.

[647] Para uma discussão mais detida, ver A. Michael Froomkin (1999) Legal Issues in Anonymity and Pseudonymity, *The Information Society: An International Journal*, 15:2, 113-127.

[648] CAPANEMA, Walter Aranha. *O direito ao anonimato:* uma nova interpretação do art. 5o, IV, CF. Disponível em: <http://www.avozdocidadao.com.br/images_02/artigo_walter_capanema_o_direito_ao_anonimato.pdf>. Acesso em: 28 nov. 2017.

[649] Disponível em: <https://policyreview.info/tags/right-non-tracking>. Acesso em: 28 out. 2017.

elucidado, todas as abordagens de anonimização na IoT contam com vantagens e desvantagens.

Independentemente, ao passo em que o avanço tecnológico requer adaptações do ordenamento jurídico aos novos cenários, inclusive de atividade interpretativa, nem sempre essas soluções são eficazes dado a forma acelerada de modificação sócio-tecnológica. Exploraremos, portanto, no item seguinte, alternativas voltadas ao aumento do controle que os usuários da Internet podem possuir sobre seus próprios dados.

2.5.2
O Modelo *"Human-Centered Personal Data"* ou "Personal Data Economy"

Como vimos ao longo deste capítulo, os dados gerados através do uso desses inúmeros dispositivos inteligentes são coletados e armazenados pelas empresas, as quais nem sempre agem de forma transparente. Os termos de uso e de serviço costumam ser extremamente técnicos e ininteligíveis para a população em geral. Não é raro que a finalidade destinada aos dados seja escondida dos próprios usuários, os quais não possuem controle sobre as informações que se referem a eles próprios.

Com o desenvolvimento da Internet das Coisas, a quantidade de dados coletada pelas instituições tem aumentado drasticamente e nos deixa mais preocupados com privacidade, confidencialidade, segurança e confiança. Todos os dados que produzimos sobre nós na Internet são coletados por alguém. Os dados pessoais, como o que lemos, o que compramos e as músicas que ouvimos, serão usados por empresas para orientar sua política de mercado para nossos desejos e hábitos, de acordo com a maneira como nos comportamos, através de técnicas como o *tracking*, *profiling e targeting*.

Diante da volumosa quantidade de dados produzida diariamente, isso se torna preocupante. O *Big Data*[650] vai muito além de um emaranhado de dados. Ele é essencialmente relacional. Os indivíduos não possuem controle de seus próprios

[650] *Big Data* é um termo em evolução que descreve qualquer quantidade volumosa de dados estruturados, semiestruturados ou não estruturados que têm o potencial de ser explorados para obter informações.

dados pessoais, que pertencem àqueles que os coletam, criando uma relação vertical. É preciso termos em mente que o *Big Data* somos nós e, portanto, devemos ter uma consciência crítica sobre isso e pensar sobre possibilidades de retomar o controle sobre nossos dados pessoais.

Dessa forma, as discussões relativas ao direito à privacidade estão intrinsecamente conectadas às discussões sobre o uso e gerenciamento de dados. O avanço tecnológico requer adaptações do ordenamento jurídico aos novos cenários, o que pode se dar, por exemplo, através da atuação legislativa ou da atividade interpretativa.

Porém, nem sempre essas soluções são eficazes: de um lado, a conjuntura sociopolítica e o padrão tecnológico mudam de forma muito mais acelerada do que a legislação é capaz de acompanhar e, de outro, a interpretação judicial e dos governantes pode adquirir caráter paternalista e corporativo se distanciando da vontade dos indivíduos.

Assim, novas formas de proteger o direito à privacidade e de aumentar o controle que os usuários da Internet possuem sobre seus próprios dados têm surgido como alternativa. As formas alternativas de lidar com os dados pessoais, conforme veremos, permitem que o indivíduo retome o controle de seus dados e os organizem de modo mais proveitoso e significativo para si mesmo.

Neste sentido, foram criados projetos como o Digital Me, o Hub of All Things (HatDex) e o My Data. Tratam-se, basicamente, de sistemas cujo objetivo é colocar o indivíduo no centro dos dados pessoais a fim de que eles próprios tenham o controle das informações produzidas sobre si, desvencilhando-se do controle abusivo exercido atualmente pelas empresas.

Vale dizer, adota-se perspectiva centrada no ser humano, e não mais nas coisas ou nas informações em si. No atual modelo de gerenciamento, os próprios indivíduos aos quais as informações se referem não têm acesso a elas e sequer sabem a finalidade para a qual elas são usadas, o que cria sérios problemas à privacidade e vai de encontro ao princípio da transparência.

Os novos sistemas elaborados buscam, assim, criar um cenário em que os usuários tenham seus direitos humanos respeitados no ambiente digital e que possam ter controle sobre seus dados ao mesmo tempo em que não sejam criadas barreiras à inovação das empresas, as quais poderão desenvolver serviços inovadores com base na confiança mútua.

A interação online é constante e está presente na vida de quase todos os indivíduos. No mundo contemporâneo hiperconectado, a obtenção de informações e notícias ocorre, cada vez mais, por meio da Internet. A contratação de produtos e serviços, assim como o estabelecimento de contratos sociais e profissionais se dão, crescentemente, por meio digital, como redes sociais e afins.

Isso, porém, muitas vezes, passa despercebido pelos usuários, que não percebem o rastro digital que produzem sobre si próprios. Os dados produzidos, não raro, são armazenados por um longo período de tempo. O controle deste rastro tem se tornado um problema tecnológico e social, já que de sua análise é possível obter informações sobre o comportamento, as preferências e necessidades pessoais de uma determinada pessoa e até mesmo prever suas ações futuras[651].

Um exemplo ligado à previsão de ações futuras das pessoas com base em seus hábitos de compra que demonstra o perigo do uso livre das informações pessoais é o cruzamento de dados feitos por empresas de venda. A Target cria uma identidade de cada consumidor por meio de informações obtidas quando o cliente usa o cartão de crédito, um cupom promocional, entra em contato com o SAC ou visita a loja online. A empresa percebeu que se uma mulher compra alguns itens em conjunto ou em maior quantidade, como loções sem cheiro, loções de manteiga de coco, suplementos com zinco e magnésio e uma bolsa grande, há 87% de chance de ela estar grávida há três meses[652].

Um caso interessante ocorreu em 2012 quando a empresa entregou, por Correio, cupons de desconto à produtos como fraldas e cremes para prevenção de estrias a uma adolescente que ainda não sabia estar grávida. Ao recebê-los, seu pai ficou furioso e processou a empresa. Entretanto, poucos meses depois, a previsão foi confirmada.[653]

---

[651] SJÖBERG, Mats et al. Digital Me: Controlling and Making Sense of My Digital Footprint. In: GAMBERINI, L. et al (Eds.). *Symbiotic Interaction*: Lecture notes in computer science. Padua: Springer, 2016, p. 155-156.

[652] RODRIGUES, Alexandre; SANTOS, Priscilla. A ciência que faz você comprar mais. *Galileu*, [s.d.]. Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI317687-17579,00-A+CIENCIA+QUE+FAZ+VOCE+COMPRAR+MAIS.html>. Acesso em: 25 set. 2017; REDAÇÃO. Varejista norte-americana descobre até gravidez de clientes com a ajuda de software. *Olhar Digital*, fev. 2012. Disponível em: <https://olhardigital.com.br/noticia/varejista-norte-americana-descobre-gravidez-de-clientes-com-a-ajuda-de-software/24231>. Acesso em: 25 set. 2017.

[653] DUHIGG, Charles. How companies know your secrets. *The New York Times*, fev. 2012. Disponível em: <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp>. Acesso em: 25 set. 2017.

Não bastasse essa coleta de dados acerca dos indivíduos e a formação de perfis individuais, os indivíduos não costumam ter acesso aos dados pessoais sobre eles gerados. As grandes empresas da Internet, como Google e Facebook, centralizam as informações coletadas e incentivam as pessoas a utilizarem apenas suas ferramentas, já que não há compartilhamento de informações entre elas - o que vai de encontro à concorrência no mercado e à inovação. O usuário não controla seus dados pessoais.[654][655]

Uma das soluções técnicas[656] recentemente propostas para este problema, aponta para dados pessoais centrados no ser humano, ou seja, com a possibilidade dos próprios indivíduos controlarem seus dados.

A iniciativa Digital Me[657] ("DiMe"), por exemplo, consiste em um "sistema de armazenamento que coleta o rastro digital do indivíduo a partir de dispositivos informáticos pessoais e cujo design tem o objetivo de permitir diferentes tipos de *machine learning* e aplicativos de processamento de informações para operar no repositório privado de dados controlado pelo usuário"[658].

O sistema mistura a manipulação interativa com a análise automatizada, para que grandes quantidades de dados pessoais sejam eficientmente gerenciadas[659]. Ele pode ser aplicado em diversos cenários de gerenciamento de dados pessoais e está disponível online como software livre e de código aberto[660].

Conforme consta na página do projeto:[661][662]

---

[654] SJÖBERG. Op. Cit., p. 155-167.
[655] SJÖBERG. Op. Cit., p. 155-167.
[656] É necessário destacar que a novidade consiste na solução técnica. O autogerenciamento da privacidade através do *notice and consent* é um sistema que já existe há décadas, mas tem se mostrado ineficaz. O que parece ser mais eficaz – ou pelo menos promissor – é, portanto, um autogerenciamento técnico.
[657] http://hiit.github.io/dime-server/.
[658] Lê-se no original: "*DiMe is a personal data storage system, which collects the individual's digital footprint from personal computing devices, and whose design is focused on enabling different kinds of machine learning and information processing applications to operate in the user-controlled private data repository*". Ibid., p. 2.
[659] Ibid., p. 155-167.
[660] Disponível em: <http://reknow.fi/dime>. Acesso em: 20 out. 2017.
[661] Disponível em: <http://hiit.github.io/dime-server/>. Acesso em: 20 out. 2017.
[662] Tradução livre do autor. No original: *The idea of the Digital Me (DiMe) server is to collect your personal data from various loggers into a central place that you control. You can run DiMe in your local machine or in a dedicated server. The DiMe server source code is open source software distributed under the GNU Affero General Public Licence (AGPL) Version 3.*

> A ideia do servidor Digital Me (DiMe) é coletar seus dados pessoais de vários *loggers* para um local central que você controla. Você pode executar o DiMe em sua máquina local ou em um servidor específico para isso. O código fonte do servidor DiMe é um software de código aberto distribuído sob a Licença Pública Geral GNU Affero (AGPL) Versão 3.

Os pesquisadores que desenvolveram o DiMe pontuam que duas abordagens principais foram propostas para permitir o controle de dados pessoais centrado no ser humano: 1) o primeiro consiste em centralizar o armazenamento dos dados em si; 2) o segundo, em concentrar-se no gerenciamento dos fluxos de dados entre fontes e usuários de dados[663] – o indivíduo controla o uso de dados pessoais, que é a lógica do modelo *MyData*, o qual será explorado mais abaixo.[664]

Apesar de o *Digital Me* centralizar o armazenamento de dados, há diferenças em relação a outros *personal data storage* (PDS), pois: 1) o desenvolvimento do DiMe está focado na integração com um amplo conjunto de *loggers* que acompanham o rastro digital; e 2) o DiMe fornece uma camada de representação para eventos de dados focada em fornecer soluções de *machine learning*, estruturar e conectar diferentes dados[665].

O DiMe fornece uma interface programática (API) para dois tipos de clientes: *loggers* (componentes de software (ou hardware + software) que gravam eventos relacionados às ações ou ambiente de uma pessoa e enviam-nas para serem armazenadas no próprio servidor DiMe da pessoa e aplicações (utilizam os eventos armazenados no DiMe pelos registradores. Normalmente, apresentam ao usuário uma interface de uso gráfica, onde uma parte dos dados é visualizada e pode ser manipulada, ou a visão dos dados pode ser modificada)[666].

Através do painel de ferramentas, o usuário sempre pode se deslogar do DiMe, excluir os eventos já gravados e escolher quais dados compartilhar. Os componentes essenciais do núcleo do software DiMe são a interface API, o banco de dados, o mecanismo de pesquisa e a estrutura de extração de recursos[667].

Um dos principais diferenciais no design do *Digital Me* é o fato de incluir capacidades de modelagem baseadas em *machine learning* de ponta desde o início, cujos algoritmos devem ser executados no próprio servidor central do

[663] SJÖBERG. Op. Cit., p. 158-159.
[664] Disponível em: <http://hiit.github.io/dime-server/>. Acesso em: 20 out. 2017
[665] Ibid., p. 159.
[666] Ibid., p. 159-160.
[667] Ibid., p. 160-161.

DiMe ou externamente, através da API[668].

O DiMe oferece uma memória digital que pode fornecer informações sobre o próprio comportamento da pessoa e pode ser usada em diferentes aplicativos. Observe que representações e *tags* de vetores são recursos para aplicativos. Há, também, exemplos de aplicações, como pesquisa em linha do tempo, recall associativo, busca proativa, sala de reuniões inteligente, pesquisa de perfil e competência[669].

A memória digital criada através do DiMe fica contida nessa plataforma, que, por sua vez, é controlada pelo indivíduo a quem a memória se refere. Isso contribui para combater os perigos associados às já mencionadas técnicas de *tracking*, *profiling e targeting*, uma vez que caberá ao próprio usuário decidir a destinação conferida a esta memória, evitando o uso indevido e desprovido de consentimento consciente por parte das empresas.

A ideia do modelo não é simplesmente reunir os dados, porque os indivíduos devem poder compreender seus próprios dados com sistemas que são capazes de organizá-los e visualizá-los.

Portanto, entre as várias maneiras de gerenciar dados pessoais, alguns pesquisadores focam em duas abordagens complementares[670]: 1) representações vetoriais geradas automaticamente: "utilizam técnicas de *machine learning* de última geração para criar representações vetoriais altamente expressivas de forma automatizada sem supervisão"[671]. Além disso, elas podem ser usadas para aprender relacionamentos semânticos e visualizar a estrutura das informações coletadas ou ajudar a encontrar eventos ou documentos relacionados; e 2) modelagem interativa de etiquetas (*tags*): busca incluir o indivíduo no ciclo de organização de dados através da utilização de *tags*, que consistem em palavras ou frases-chave para classificar os eventos ou documentos coletados.

O sistema é capaz de aprender as categorizações utilizadas pelo indivíduo e classificar os novos eventos sozinho, organizando todo o rastro digital. Interessante notar que "com o padrão de design de marcação convencional, as etiquetas rotulam os eventos como sendo mapeados em várias categorias

[668] Ibid., p. 162.
[669] Ibid., p. 165-166.
[670] Ibid., p. 165-166.
[671] Ibid., p. 162.

potencialmente sobrepostas em vez do sistema de categoria hierárquica tradicional comumente utilizado, por exemplo, em sistemas de arquivos"[672].

Apesar de ser um projeto ainda em desenvolvimento, o DiMe representa uma potencial solução para que usuários possam entender como ter controle sobre o seu rasto digital além de proteger os seus dados pessoais.

Outra interessante iniciativa é o Projeto HATDEX. Procurando por uma solução para a economia digital voltada à inovação, um grupo formado por pesquisadores de seis universidades[673] desenvolveu o projeto *Hub of All Things* (HAT), fundado pelo Programa de Economia Digital do Conselho de Pesquisa do Reino Unido.

O HAT é uma plataforma de dados pessoais que vai além de um local seguro para armazenar dados: ele é o próprio assistente de dados pessoais. Através dele, as pessoas podem reivindicar seus dados, combiná-los e organizá-los de forma criativa e da maneira que considerem mais pertinente.

Além disso, os indivíduos têm o poder de controlar com quem irão compartilhar seus dados e podem analisar suas próprias informações, o que lhes permite atuar de modo mais inteligente. A combinação dos dados e o recebimento de informações sobre cada um dos indivíduos e serviços permite que sejam criados aplicativos e dispositivos conectados específicos, que ajudarão as pessoas a coletar e analisar seus próprios dados.

Através do HAT é colocada à disposição do usuário um *marketplace* para seus dados pessoais, com as seguintes vantagens atreladas aos dados presentes no aplicativo da plataforma:[674]

> (i) eles são armazenados em um único lugar;
> (ii) são de propriedade do indivíduo; e
> (iii) fornecem uma imagem detalhada de como usam, experimentam e consomem produtos e serviços.

O HAT cria um tipo de banco de dados horizontal, afastando o problema da verticalidade da relação. Ou seja, os dados não estão mais numa relação hierárquica em que os usuários deixam de ser donos destes e passam a ser meras

[672] Ibid., passim.
[673] Os pesquisadores são de Universidades do Reino Unido: de Cambridge, Edimburgo, Nottingham, Surrey, Warmick e Oeste da Inglaterra.
[674] Disponível em: <https://hubofallthings.com>. Acesso em: 20 out. 2017.

fontes de informações e objeto do direcionamento de marketing. Por meio desse modelo, eles passam a ter controle dos dados que produzem sobre si mesmos e a definir quem terá acesso a eles, bem como as finalidades que lhes serão conferidas.

A compreensão sobre o significado dos dados requer contextualização, e, com isso, eles começam a se tornar valiosos para os indivíduos. Os dados são organizados de forma que ajudam a maneira como vivemos nossas vidas. As empresas poderão, desta maneira, desenvolver produtos que sejam mais úteis e oferecer melhores serviços de acordo com o que os indivíduos desejam compartilhar com elas.

Ao criar uma plataforma horizontal que se adapta às vidas humanas, a próxima etapa da Internet também é criada: a das pessoas e das coisas. Além disso, cria-se a possibilidade do desenvolvimento de novos modelos comerciais e econômicos de tipo horizontal centrados no ser humano – que em breve surgirão.

A ideia é que o repositório de dados horizontais e significativos deixe os indivíduos decidirem se querem negociar ou trocá-los com as empresas por produtos e serviços e também os ajude a tomar decisões através da integração e contextualização das ferramentas. Nesse sentido, o HAT é uma plataforma de código aberto.

Uma vez que todos os dados sobre um indivíduo estão localizados em um único lugar, é importante ter atenção à segurança. Existe um projeto adjacente que está desenvolvendo um sistema de segurança distribuído que permite que os dados que o indivíduo possui permaneçam onde estão (por exemplo, dados da universidade), bem como que fiquem integrados em um local onde é possível visualizá-los[675].

A tecnologia da plataforma HAT pode ser explicada em seis partes. Primeiro, o HAT é uma plataforma aberta[676]. É facilmente adaptável para qualquer aplicação personalizada, está evoluindo continuamente para maior controle e funcionabilidade, entre outras coisas.

Em segundo lugar, há um painel de controle para visualizar todas as

[675] Uma análise aprofundada sobre o projeto de segurança fugiria do escopo deste artigo. Mais informações podem ser conferidas. Disponível em: <http://nymote.org/>. Acesso em: 27 fev. 2017.
[676] Disponível em: <https://hubofallthings.com>. Acesso em: 20 out. 2017.

informações no HAT: o RUMPEL[677]. Entre suas funcionalidades, os usuários podem gerenciar a conexão de dados (*data plug*) e rastrear dados recebidos de vários serviços e aplicativos. Além disso, podem procurar suas localizações a partir do ponto em que conectaram os dados locais. Ele permite que o usuário visualize e customize toda a sua informação contida no HAT.

Em terceiro lugar, o DEX (*data exchange*)[678], integrante do sistema HAT, é um serviço que consiste em: i) processos de troca de dados; ii) registro de transações de dados e estatísticas em todo o ecossistema; e iii) *HAT Access*: mediação para aplicativos e desenvolvedores. "Esses processos registram todas as atividades no ecossistema HAT, respondem aos pedidos para criar *Data Debits*, instalam os *Data Plugs*, mantém transações de dados, verificam trocas e enviam e recebem dados entre as partes de forma rápida, precisa e segura"[679]. Ainda, relata as estatísticas do ecossistema, bem como a integração de conjuntos e serviços de dados para terceiros no sistema.

O outro aspecto é o mercado (*marketsquare*)[680], onde é permitido que os indivíduos comprem e vendam aplicativos HAT, ofereçam dados (pode-se comprar e vender dados autorizados) e outros bens e serviços no mercado habilitado para o sistema. Os desenvolvedores e os empresários podem aprender a hospedar novas aplicações HAT, as empresas podem colocar suas ofertas de dados para o público e os indivíduos podem acessar aplicativos e ofertas personalizadas.

Além disso, há envolvimento e apoio da comunidade. O *DataBuyer* é o "próprio centro de dados da *MarketSquare*, baseado na confiança, na transparência e na privacidade do usuário. Marcas, departamentos governamentais, organizações e universidades podem usar o *DataBuyer* para configurar ofertas de dados, solicitando dados específicos dos usuários em troca de serviços, recompensas, descontos ou mesmo dinheiro.

A estrutura de troca de dados em que o *DataBuyer* é construído significa que apenas os dados solicitados são recebidos, permitindo que os usuários se mantenham completamente anônimos e sua privacidade seja garantida em todos

[677] Disponível em: <https://marketsquare.hubofallthings.com/c/apps/rumpel>. Acesso em: 20 out. 2017.
[678] Disponível em: <http://developers.hubofallthings.com/guides/dex>. Acesso em: 20 out. 2017.
[679] Idem.
[680] Disponível em: <https://marketsquare.hubofallthings.com>. Acesso em: 20 out. 2017.

os momentos. O *DataBuyer* é um mercado aberto, onde usuários com HATs podem descobrir ofertas criadas por várias organizações, reivindicar os benefícios que oferecem ao compartilhar seus dados e contribuir ativamente para a economia de troca de dados"[681].

Por fim, o *HAT Milliner Service*[682] é o software de implantação HAT usado no *HATs-on-Demand* e *HATs-as-a-Service*. Seu objetivo é conferir dinamicidade na implantação do HAT. Assim, oferece armazenamento padrão para cada HAT, mecanismo para iniciá-lo e gerenciá-lo e regras para backup e recuperação do HAT.

Para indivíduos (pessoas físicas), já é possível fazer o *download* do aplicativo (*HAT – Hub-of-All-Things)* para celular. A partir do download do aplicativo, é possível criar uma conta, facilitando a forma de organizar dados pessoais e passando a exercer maior controle sobre o compartilhamento dos seus dados. As informações utilizadas para criar uma conta (nome, sobrenome e e-mail) são apenas para esse fim – criar uma conta no HAT -, e não são compartilhadas a não ser que o indivíduo autorize tal compartilhamento. Cada indivíduo tem um *username* para identificar a sua conta e, por meio dele, todos os usuários do HAT podem se encontrar.

Uma outra iniciativa vale menção em complemento àquelas analisadas, conhecida como MY DATA. [683] O MyData consiste em uma estrutura com sistema centrado no ser humano e baseada no auto-gerenciamento de dados. O Projeto baseia-se na ideia de que os indivíduos devem estar no centro do controle de seus próprios dados e seus direitos humanos digitais devem ser fortalecidos ao mesmo tempo em que as empresas têm a possibilidade de desenvolver serviços inovadores baseadas na confiança mútua[684].

A abordagem de infraestruturas interoperáveis do MyData fornece aos indivíduos serviços baseados em dados permitindo uma auto-coordenação do tratamento de dados pessoais, com maior privacidade e transparência, aumentando

[681] Disponível em: <https://marketsquare.hubofallthings.com/c/apps/data-buyer>. Acesso em: 20 out. 2017.
[682] Disponível em: <http://www.hatdex.org/hat-milliner-service>. Acesso em: 20 out. 2017.
[683] POIKOLA, Antti; KUIKKANIEMI, Kai; HONKO, Harri. MyData - A Nordic Model for human-centered personal data management and processing. *Ministry of Transport and Communications*, [s.d.], p. 3. Disponível em: <https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/>. Acesso em: 28 set. 2017.
[684] Ibid., p. 1.

a liberdade de escolha e empoderando o usuário. A gestão de consentimento é o principal mecanismo para permitir e aplicar o uso legal de dados segundo esta iniciativa. Nesse modelo, os consentimentos são dinâmicos, mais fáceis de compreender, legíveis por máquina, padronizados e gerenciados de forma coordenada. [685]

O objetivo do MyData é justamente fazer com que indivíduos possam acessar e fazer uso de conjuntos de dados que contenham suas informações pessoais, como por exemplo, registros médicos ou informações financeiras. Busca-se incentivar organizações detentoras de dados pessoais a transferir aos indivíduos o controle sobre esses dados.

O MyData, portanto, equipa os indivíduos para controlar quem usa seus dados pessoais, estipular para quais fins podem ser usados e dar consentimento informado de acordo com os regulamentos de proteção de dados pessoais. Os fluxos de dados tornam-se mais transparentes, abrangentes e gerenciáveis. Os usuários também podem desativar fluxos de informações e retirar o consentimento. Por fim, os consentimentos legíveis por máquina podem ser visualizados, comparados e processados automaticamente[686].

Além disso, o MyData pode ser considerado útil para as empresas, porque ajudará a integrar serviços complementares de terceiros em seus serviços principais; simplificará as operações dentro dos marcos regulatórios atuais e futuros e permitirá o uso de dados para fins exploratórios; e possibilitará a criação de novos negócios com base no processamento e gerenciamento de dados. [687]

É interessante notar que o MyData é complementar ao *Big Data* e vice-versa, porque, sem abordar a perspectiva humana, muitos dos potenciais usos inovadores do *Big Data* são incompatíveis com os regulamentos e regulações atualmente em vigor.

Essa abordagem tem três princípios que requerem maturação: **(i) controle sobre os dados centrado no ser humano**: o ser humano é um ator ativo na gestão de sua vida online e offline e "tem o direito de acessar seus dados pessoais e

[685] Ibid., p. 7.
[686] Ibid., p. 8.
[687] Ibid., p. 8.

controlar suas configurações de privacidade"[688], tanto quanto seja necessário para efetivá-los; **(ii) dados utilizáveis**: é necessário que os dados pessoais sejam tecnicamente fáceis de acessar e legíveis pelas APIs (*Application Programming Interfaces*). O MyData converte dados em um recurso reutilizável para criar serviços que ajudam os indivíduos a gerenciar suas vidas; e **(iii) ambiente de negócios aberto**: a infraestrutura permite o gerenciamento descentralizado de dados pessoais, melhora a interoperabilidade, facilita a conformidade das empresas com os regulamentos de proteção de dados e permite que os indivíduos troquem os provedores de serviços sem bloqueio de dados.

Assim, "ao cumprir um conjunto comum de padrões de dados pessoais, as empresas e os serviços permitem que as pessoas exerçam a liberdade de escolha entre serviços interoperáveis", evitando que as pessoas tenham seus dados bloqueados em "serviços pertencentes a uma única empresa porque não podem exportá-los" e levá-los para outro provedor[689]. (grifos nossos)

As vantagens e possibilidades que se abrem para os indivíduos foram destacadas por Doc Sealrs: [690]

> a) Gerenciar relacionamentos com organizações;
> b) Fazer com que os indivíduos sejam os centros de coleta de seus próprios dados, de modo que históricos de transações, registros de saúde, detalhes de associação,

[688] Tradução livre. Lê-se no original: "*people have a right to access their personal data and control their privacy settings, as well as the means necessary to enact these rights*". BELLI, Luca; SCHWARTZ, Molly; LOUZADA, Luiza. Selling your soul while negotiating the conditions: from notice and consent to data control by design. *Health Technology*, 2017, p. 8. Disponível em: <https://link.springer.com/article/10.1007/s12553-017-0185-3>. Acesso em: 28 set. 2017.

[689] Tradução livre. Lê-se no original: "*by complying to a common set of personal data standards, business and services make it possible for people to exercise freedom of choice between interoperable services, preventing the current scenario where people get 'locked' into silos of services owned by a single company because they cannot export their data and take it elsewhere*". BELLI; SCHWARTZ; LOUZADA, op. cit., p. 8.

[690] Tradução livre. Lê-se no original: "*a) Manage relationships with organizations; b) Make individuals the collection centers for their own data, so that transaction histories, health records, membership details, service contracts, and other forms of personal data are no longer scattered throughout a forest of silos; c) Give individuals the ability to share data selectively, without disclosing more personal information than the individual allows; d) Give individuals the ability to control how their data is used by others and for how long. At the individual's discretion, this may include agreements requiring others to delete the individual's data when the relationship ends; e) Give individuals the ability to assert their own terms of service, reducing or eliminating the need for organization-written terms of service that nobody reads and everybody has to 'accept' anyway; f) Give individuals means for expressing demand in the open market, outside any organizational silo, without disclosing any unnecessary personal information; g) Base relationship-managing tools on open standards, open APIs (application program interfaces), and open code; h) Make relationships work both ways*". SEALRS, D. *The intention economy*: when customers take charge. Cambridge: Harvard Business Review Press, 2012 *apud* BELLI; SCHWARTZ; LOUZADA. op. cit., p. 8-9.

> contratos de serviços e outras formas de dados pessoais não sejam espalhados por uma floresta de silos;
> c) Conferir aos indivíduos a capacidade de compartilhar dados seletivamente, sem divulgar mais informações pessoais do que o indivíduo permite;
> d) Conferir aos indivíduos a capacidade de controlar como seus dados são usados por outros e por quanto tempo. A critério do usuário, isso pode incluir acordos que exigem que outros excluam os seus dados quando o relacionamento termina;
> e) Conferir aos indivíduos a capacidade de fazer valer seus próprios termos de serviço, reduzindo ou eliminando a necessidade de termos de serviço por escrito organizados que ninguém lê e todos devem "aceitar" de qualquer maneira;
> f) Conferir aos indivíduos meios para expressar suas demandas no mercado aberto, fora de qualquer silo organizacional, sem divulgar informações pessoais desnecessárias;
> g) Possuir ferramentas básicas de gerenciamento de relacionamento em padrões abertos, APIs abertas (interfaces de programas de aplicativos) e código aberto;
> h) Fazer com que os relacionamentos sejam trabalhados em ambos os sentidos."

O MyData é uma infraestrutura mais robusta diante das Interfaces de Programação de Aplicativos ("APIs")[691] que usualmente acessamos. O agregador de dados comumente usado hoje em outras plataformas está evoluindo naturalmente para fora da economia da API, mas apresenta desvantagens importantes: a falta de interoperabilidade entre os agregadores de dados e o fato de que a atual fonte dos agregadores não reconhece necessariamente a privacidade como um valor a ser garantido ou não se envolve em uma relação transparente com os indivíduos.

A adoção da abordagem do MyData pode levar a uma simplificação sistêmica do ecossistema de dados pessoais e essa simplificação pode ser feita gradualmente, pois a plataforma pode ser desenvolvida e implantada em estágios, ao lado da evolução da economia da API e do modelo de agregador de dados existente[692].

Finalmente, é interessante observar como funciona a arquitetura do MyData: baseia-se em contas interoperáveis e padronizadas: [693]

---

[691] "API é um conjunto de rotinas e padrões de programação para acesso a um aplicativo de software ou plataforma baseado na Web. A sigla API refere-se ao termo em inglês "Application Programming Interface" que significa em tradução para o português "Interface de Programação de Aplicativos". Disponível em: https://canaltech.com.br/software/o-que-e-api/. Acesso em: 28 set. 2017.

[692] POIKOLA, Antti; KUIKKANIEMI, Kai; HONKO, Harri. MyData - A Nordic Model for human-centered personal data management and processing. *Ministry of Transport and Communications*, [s.d.], p. 6. Disponível em: <https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/>. Acesso em: 28 set. 2017.

[693] Ibid., p. 6.

> O modelo fornece aos indivíduos uma maneira fácil de controlar seus dados pessoais de um único lugar, mesmo que os dados sejam criados, armazenados e processados por centenas de serviços diferentes. Para desenvolvedores, o modelo facilita o acesso a dados e remove a dependência de agregadores de dados específicos. As contas geralmente serão fornecidas por organizações que atuam como operadores MyData. Para organizações ou indivíduos dispostos a ser independentes do operador, também será tecnicamente possível hospedar contas individuais, assim como algumas pessoas atualmente optam por hospedar seus próprios servidores de e-mail.

A interoperabilidade é a principal vantagem proporcionada pelo MyData, mas também é o principal desafio, porque requer maior padronização, mais redes de confiança e formatos de dados. Em sua arquitetura, os dados fluem de uma fonte de dados para um serviço ou aplicativo. A função principal de uma conta MyData é habilitar a gestão do consentimento. APIs permitem a interação entre fontes e usuários de dados[694]. Como já mencionado, a arquitetura padronizada torna as contas interoperáveis e permite que os indivíduos troquem facilmente de operadores.

A título de exemplo, o MyData tem sido utilizado na área de saúde, tendo como inciativa o projeto *Digital Health Revolution*[695]. Dados clínicos e registros médicos contêm dados sensíveis como resultados de testes e diagnósticos e, tendo em vista que prestadores de cuidado de saúde ocupacional mudam na medida em que indivíduos mudam de empregos, as informações deste acabam sendo transferidas.

Logo, o MyData seria uma forma de agrupar essas informações sensíveis, otimizando os serviços relacionados a saúde, sendo possível providenciar métodos alternativos para diagnóstico. A infraestrutura oferecida pelo MyData ajudaria na gestão e na logística desses dados.

Os objetivos do projeto *Digital Health Revolution* incluem uma contribuição para a mudança no controle de dados a favor do indivíduo, desenvolver movimentos bem-sucedidos de dados pessoais em todos os sistemas e serviços, além de criar um ecossistema MyData.

Em agosto/setembro de 2017, o MyData promoveu uma conferência[696],

---

[694] POIKOLA, Antti; KUIKKANIEMI, Kai; HONKO, Harri. MyData - A Nordic Model for human-centered personal data management and processing. *Ministry of Transport and Communications*, [s.d.], p. 8. Disponível em: <https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/>. Acesso em: 28 set. 2017

[695] Disponível em: <http://www.digitalhealthrevolution.fi/>. Acesso em 28 set. 2017.

[696] Disponível em: <https://mydata2017.org/presentations/>. Acesso em: 28 set. 2017.

onde foram apresentados *Case Studies* e projetos de pessoas que utilizaram o aplicativo de forma prática. Um desses projetos, apresentado por Anna Rizzo[697], teve como foco essa questão de dados relacionados a saúde – *My Health, My Data* (MHMD).

O MHMD é um projeto financiado em parte pela União Europeia, que busca desenvolver uma plataforma para o compartilhamento e troca de dados pessoais relacionados à saúde entre instituições clínicas, indivíduos, centros de pesquisa e indústrias voltadas para cuidados médicos. Além disso, os dados em comento também servem para fins de pesquisa.

O objetivo principal é conceder aos indivíduos a propriedade e controle sobre seus dados pessoais de saúde. Para tanto, são usadas diferentes abordagens[698], como por exemplo: 1) Blockchain: a tecnologia blockchain é segura e verificável quando se trata de transações na Internet. Todas as transações são confirmadas pela rede, além de serem constantemente monitoradas em termos de legitimidade. "A aplicação da tecnologia blockchain para dados de saúde garante um acesso seguro de qualquer lugar em qualquer dispositivo"; 2) Smart Contracts: contratos auto executáveis, com base na formalização de relações contratuais em formato digital, que automatizam a execução de transações em condições definidas pelo usuário - o que se adequa a nova regulação de dados pessoais, GDPR[699], que entrará em vigor em maio deste ano; e também através do 3) Data Catalogue: por meio do qual se busca dados específicos para fins específicos.

De modo contrário, o atual modelo pelo qual os dados pessoais são geridos de maneira geral pelas outras plataformas vai de encontro ao direito à privacidade e à transparência, além de reduzir o poder de escolha dos indivíduos. Os termos de uso dos serviços online oferecidos pelas empresas são longos a ponto de desincentivar a leitura por parte do usuário e possuem termos técnicos não inteligíveis pela população sem conhecimentos tecnológicos específicos. O

[697] Ibid.
[698] Ibid., p. 7-13.
[699] Disponível em: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr>. Acesso em: 28 set. 2017.

mesmo ocorre com as políticas de privacidade.[700]

Uma pesquisa feita em 2017 por professores das Universidades de Michigan e de Connecticut[701] envolveu participantes e mostrou que 74% dos usuários não lêem as políticas de privacidade. Aqueles que o fazem gastam, em média, apenas 74 segundos nessa tarefa. O tempo médio gasto para a leitura dos termos de serviço é de 51 segundos.

Para Aleecia McDonald e Lorrier Cranor[702], o tempo de leitura das políticas de privacidade é uma forma de pagamento. A leitura de todas as políticas levaria, anualmente, 201 horas e equivaleria a $3.534 por ano, por cada usuário americano. Sob a perspectiva nacional, a leitura detida dessas políticas faria com que o tempo gasto equivalesse a cerca de $781 bilhões anualmente.[703]

As pessoas não sabem o valor que seus dados possuem e, na maioria das vezes, não querem lidar com a complicação de gerenciá-los[704]. Com isso, as empresas utilizam os dados da forma que lhes parece mais interessante, o que pode envolver a venda e a transferência das informações para terceiros, aumentando os riscos de vazamento e, portanto, de violação da privacidade.

O fato de os dados serem não-rivais, isto é, poderem ser usados ao mesmo tempo por mais de uma pessoa ou algoritmo, cria complicações, como dar-lhes destinação distinta daquela à qual o usuário manifestou consentimento. Neste cenário, os dados pertencem àqueles que os coletam, e não à pessoa a quem eles se referem.

Pesquisadores[705] do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas fizeram um estudo comparando 50 termos de uso e serviço de

[700] Belli, L., Schwartz, M., & Louzada, L. (2017). Selling your soul while negotiating the conditions: from notice and consent to data control by design. *Health Technology*. Retrieved from https://link.springer.com/article/10.1007/s12553-017-0185-3

[701] OBAR, J. A.; OELDORF-HIRSCH, A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. In: *The 44th Research Conference on Communication, Information and Internet Policy*, 2016, p. 10-22. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465>. Acesso em: 28 set 2017.

[702] MCDONALD, A. M.; CRANOR, L. F. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, v. 4, n. 3, p. 543-568, 2008.

[703] Belli, L., Schwartz, M., & Louzada, L. (2017). Selling your soul while negotiating the conditions: from notice and consent to data control by design. *Health Technology*. Retrieved from <https://link.springer.com/article/10.1007/s12553-017-0185-3>. Acesso em: 28 set. 2017

[704] DATA IS GIVING rise to a new economy. *Economist*, 6 may. 2017. Disponível em: <https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>. Acesso em: 03 jul. 2017.

[705] VENTURINI, Jamila et. al. *Terms of Service and Human Rights*: an analysis of online platform contracts. Rio de Janeiro: Revan, 2016, p. 74.

plataformas online analisando como eles lidam com os direitos humanos. Os autores concluíram que, sob essa ótica, os termos são abusivos.

O maior objetivo das empresas ao os adotarem é "minimizar a exposição à responsabilidade, mais do que detalhar sua obrigação de garantir respeito a certos direitos"[706], o que explica tanto a terminologia vaga e ambígua adotada quanto "a tendência de fornecer aos usuários o mínimo de informação possível, particularmente nos aspectos cruciais para a proteção dos direitos humanos"[707].

Neste sentido, o estudo mostrou que apenas 12% das plataformas prevêem em seus termos de uso a possibilidade de, após o cancelamento da conta, os dados pessoais gerados pelos usuários ou coletados de outra forma serem excluídos. 60% das plataformas sequer fornece informações sobre o assunto, ao passo que 10% afirmam expressamente que não permitem a exclusão total dos dados. 18% fornece informações contraditórias nesse aspecto[708].

Outro exemplo interessante consiste no fato de que 62% das empresas possuem cláusulas exigindo consentimento dos usuários para o compartilhamento dos dados com fins comerciais[709], o que nos leva a questionar se o consentimento dado pelo usuário é efetivamente informado.

Os problemas ligados à privacidade e ao gerenciamento de dados por parte das empresas nos levam a entender que o modelo de consentimento atualmente existente falhou[710]. Por esse modelo, os dados pessoais tornaram-se uma moeda que pode ser utilizada pelos indivíduos para acessar conteúdo online. Em outras palavras, para desfrutar de um serviço e não ser excluído de seu uso, o indivíduo consente que seus dados pessoais sejam acessados, processados e divulgados[711]. Observe o que lecionam Luca Belli, Molly Schwartz e Luiza Louzada: [712]

---

[706] VENTURINI, Jamila et. al. *Terms of Service and Human Rights*: an analysis of online platform contracts. Rio de Janeiro: Revan, 2016, p. 74.
[707] Ibid.
[708] Ibid., p. 47.
[709] Ibid., p. 53.
[710] É o que afirmou Eduardo Magrani em entrevista à Mobile Time: "O modelo de consentimento falhou. O fato de existir o termo de consentimento não interessa porque ninguém lê. A maioria das plataformas coleta mais dados do que o necessário para o serviço que presta, o que não faz o menor sentido. ". PAIVA, Fernando. 'O modelo de consentimento falhou', diz professor da FGV. *Mobile Time*, set. 2017. Disponível em: <http://www.mobiletime.com.br/26/09/2017/-o-modelo-de-consentimento-falhou--diz-professor-da-fgv/477582/news.aspx>. Acesso em: 29 set. 2017.
[711] BELLI; SCHWARTZ; LOUZADA. op. cit., p. 4.
[712] Tradução livre. Lê-se no original: "*Therefore, it may be argued that the N&C scheme is grounded on a series of dubious claims. Firstly, it assumes that individuals expressing their consent to PP and ToS behave as rational economic subjects, having the time and knowledge to*

> Pode-se argumentar que o esquema N&C [notice and consent] baseia-se em uma série de reivindicações duvidosas. Em primeiro lugar, assume que os indivíduos que expressam o seu consentimento para PP [Políticas de Privacidade] e ToS [Termos de Serviço] se comportam como sujeitos econômicos racionais, com tempo e conhecimento para analisar cuidadosamente o conteúdo de cada contrato. Em segundo lugar, ele postula que os indivíduos possuem o poder de barganha necessário para aceitar livremente as disposições incluídas em acordos contratuais definidos unilateralmente pelos prestadores. Tais suposições superestimam claramente tanto o poder de barganha quanto o grau, qualidade e inteligibilidade da informação à disposição das pessoas que estão pesando os custos e os benefícios de fornecer o seu consentimento".

A ineficácia dos termos de serviço e a ausência de consentimento informado ficam ainda mais claras no cenário da Internet das Coisas. Pesquisa de 2017 da Unisys Security[713] envolveu cidadãos de 13 países e mostrou que o brasileiro é o mais disposto a fornecer seus dados pessoais em troca do conforto da conectividade entre seus dispositivos[714].

A título de exemplo, 88% dos brasileiros são favoráveis à colocação de sensores nas bagagens para haver comunicação com o sistema do aeroporto, de modo que seus itens sejam localizados com mais facilidade; 83% aceitam que informações de saúde obtidas por meio de marca-passos, dentre outros dispositivos, sejam compartilhadas com médicos; e 50% concordam com o fornecimento de informações ligadas a atividades físicas obtidas por meio relógios a empresas de seguro-saúde.

O grande interesse das empresas pelos dados pessoais deve-se, sobretudo, à sua utilidade econômica, de modo que, no presente século, eles equivalem ao que o petróleo significou no século passado[715].[716] Além disso, os dados são

---

analyse carefully the content of every contractual agreement. Secondly, it postulates that individuals hold the bargaining power necessary to freely accept the provisions included in contractual agreements unilaterally defined by the providers. Such assumptions clearly overestimate both the bargaining power and the degree, quality and intelligibility of the information at the disposal of individuals who are weighing the costs and benefits of providing their consent". Ibid., p. 4.

[713] Disponível em: <http://www.unisys.com/unisys-security-index/>. Acesso em: 27 set. 2017.

[714] SOPRANA, Paula. Internet das Coisas: Brasil lidera em disposição para fornecer dados pessoais. *Época*, set. 2017. Disponível em: <http://epoca.globo.com/tecnologia/experiencias-digitais/noticia/2017/09/Internet-das-coisas-brasil-lidera-em-disposicao-para-fornecer-dados-pessoais.html>. Acesso em: 28 set. 2017.

[715] DATA IS GIVING rise to a new economy. *Economist*, 6 may. 2017. Disponível em: <https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>. Acesso em: 3 jul. 2017.

[716] A analogia com o petróleo foi divulgada no World Economic Forum de 2011. Disponível em: <http://gerdleonhard.typepad.com/files/wef_ittc_personaldatanewasset_report_2011.pdf>. Acesso em: 27 set. 2017.

transportados para milhares de computadores que extraem determinados valores, como padrões, predições e outros *insights* sobre as informações digitais dos indivíduos[717] – o que pode ser empregado nas políticas de marketing, em mecanismos de inteligência artificial e em serviços "cognitivos"[718].

Este quadro deve ser alterado. Como afirmou Elizabeth Denham, o ponto fulcral no debate sobre proteção de dados reside, sempre, na necessidade de aumentar a confiança que o público possui em relação à forma como seus dados pessoais são utilizados[719]. No atual cenário, para que o indivíduo tenha acesso a diversos produtos e serviços – por mais simples que eles sejam, como a leitura de um jornal online –, ele se vê diante da necessidade de conceder suas informações ao vendedor. Por isso, apenas se o consumidor confiar no fornecedor do produto ou do serviço é que este será capaz de implementar inovações em seu processo produtivo e nos artigos ofertados.

As informações digitais provêm de diferentes fontes e são extraídas, refinadas, valoradas, compradas e vendidas de diferentes formas. Isso muda as regras do mercado e demanda um novo *approach* regulatório[720]. É preciso que os indivíduos possuam controle sobre seus dados e tenham consciência do destino que lhes será conferido após a autorização de uso, o que, dentre outros benefícios, irá aumentar a liberdade de escolha dos usuários e os empoderará. Ademais, é preciso enfrentar o desafio de fazer com que as pessoas entendam o valor que seus dados possuem e que a elas é devida uma compensação pela concessão das informações[721].

A confiança dos usuários na regulação da privacidade e da liberdade de informação está intimamente conectada à democracia, como pontua Denham, e a economia digital é dependente daquela confiança[722]. Privacidade e inovação não

---

[717] A analogia com o petróleo foi divulgada no World Economic Forum de 2011. Disponível em: <http://gerdleonhard.typepad.com/files/wef_ittc_personaldatanewasset_report_2011.pdf>. Acesso em: 27 set. 2017.
[718] Ibid.
[719] DENHAM, Elizabeth. Promoting privacy with innovation within the law (Speech). In: 30TH ANNUAL CONFERENCE OF PRIVACY LAWS AND BUSINESS, Cambridge, 4 jul. 2017. Disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/promoting-privacy-with-innovation-within-the-law/>. Acesso em: 05 jul. 2017.
[720] DATA IS GIVING rise to a new economy. *Economist*, 6 may. 2017. Disponível em: <https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>. Acesso em: 3 jul. 2017.
[721] Ibid.
[722] DENHAM. op. cit.

precisam ser divergentes. A tarefa de desenvolver uma infraestrutura na qual estes dois elementos sejam convergentes é difícil e requer elevados níveis de dedicação.

Contudo, a tarefa, que não é impossível, é essencial: a privacidade demanda o mais alto nível de inovação[723]. É preciso que a privacidade e a inovação andem em conjunto, de forma que não se choquem e que uma não atrapalhe a evolução da outra. Elas podem e devem caminhar paralelamente. É isto que o público espera e que o Direito exige[724].

Tendo em vista estas necessidades de mudança, os projetos acima apresentados foram desenvolvidos para conferir ao indivíduo o poder sobre suas informações e fazer com que eles sejam os proprietários de seus dados – e não mais as empresas que os coletam. Projetos desse viés podem ser a solução para superar uma Internet dominada por oligopólios, técnicas de *profiling* e vigilância generalizada[725].

Todos os três partem do contexto atual de gerenciamento de dados, que é danoso à privacidade e à transparência, e buscam empoderar os indivíduos, devolvendo-lhes o controle sobre seus próprios dados. Estamos em constante interação digital e deixamos rastros a cada clique que fazemos. A maioria dessas interações são armazenadas por um longo tempo, o que cria um histórico digital das pessoas e permite analisar seus comportamentos, preferências, necessidades e até prever ações futuras.

Em geral, esses dados não estão disponíveis para os próprios usuários e eles sequer sabem quais informações estão sendo coletadas e armazenadas. Os indivíduos não controlam seus próprios dados – as empresas o fazem. Diante disso, os projetos têm um claro objetivo em comum: fazer com que as pessoas controlem seus dados e decidam, com base em informações claras e na organização útil de seus dados, se querem contratar determinado produto ou serviço.

Os sistemas que estão sendo desenvolvidos têm sua visão central focada

[723] É o que afirma CAVOUKIAN, Ann. Privacy by Design. *IEEE Technology and Society Magazine*, winter 2012, p. 19. Confira-se: "I'd also like to clear up a common misconception that privacy somehow stifles innovation. Not true! In fact, protecting privacy demands the highest level of innovation".
[724] DENHAM. op. cit.
[725] ABITEBOUL, Serge; ANDRÉ, Benjamin; KAPLAN, Daniel. Managing your digital life. *Communications of the ACM*, v. 58, n. 5, p. 35, may. 2015.

no ser humano, mas também são úteis às empresas, que poderão criar produtos e serviços mais proveitosos aos indivíduos. Um dos pontos em comum que também merece destaque é o fato de que os projetos não se limitam a propor uma reunião de dados em um único local, mas apresentam modelos pelos quais os indivíduos podem compreender e organizar seus dados, de forma a obter uma visualização mais clara e compreensível das informações constantes dos sistemas.

Nada obstante, a adesão a essas abordagens ainda é embrionária. As grandes empresas ligadas à tecnologia e ao gerenciamento de dados, como Facebook e Google, não têm interesse no avanço de projetos como esses, já que se tratam de algo extremamente disruptivo para seus modelos de negócios.

Diante disso, ao lado da maior divulgação desses projetos, é preciso pensar em formas de fazer com que os usuários se conscientizem do valor e da importância de seus dados e percebam que podem ter controle sobre eles, definindo quem irá utilizá-los, quando e para quê.

Trataremos no capítulo seguinte das problemáticas éticas desse novo mundo de dados tratados e decisões algorítmicas e de intensificação da relação entre homens e Coisas. Exploraremos, ainda, as vertentes e perspectivas éticas mais adequadas para o norteamento desse avanço tecnológico. Aprofundaremos as influências destes elementos na esfera pública conectada, buscando compreender melhor seu impacto no próprio sistema democrático, sugerindo novas lentes teóricas para uma análise mais adequada à era da hiperconectividade.

3
A ética das ‘coisas’: da ética do discurso e racionalidade comunicativa ao novo materialismo de sistemas sociotécnicos

“Technological action may be termed a form of goal-oriented human behaviour aimed at primarily resolving practical problems”

Peter Kroes

"The goal of all actions is to shape the future"

Nick Breems

Ao pretendermos discutir ética, tendo por foco, neste trabalho, o cenário de hiperconectividade da Internet das Coisas (como um cenário de entrelaçamento envolvendo o *Big Data* das pessoas, Coisas e Inteligência Artificial), temos por objetivo pensar sobre os parâmetros que nortearão nossa sociedade cada vez mais moldada pela tecnologia, com efeitos, conforme trataremos aqui, também democráticos.

O primeiro passo para essa reflexão, como demonstramos nos capítulos anteriores, consiste em termos uma consciência crítica sobre este novo mundo de dados que nos cerca, tendo em mente o valor que os nossos dados pessoais possuem no atual cenário hiperconectado e o quanto estamos sendo moldados a todo tempo em nossos comportamentos e visões de mundo por meio das esferas digitais.

Neste capítulo, pretendemos ir além de toda a problemática envolvendo a necessidade de uma regulação adequada voltada à proteção dos dados pessoais e de possíveis alternativas ferramentais aos abusos relacionados aos dados dos cidadãos. O passo seguinte, portanto, é termos dimensão da gravidade de não possuirmos ainda um norteamento ético adequado para o avanço das tecnologias digitais, seja nas fases de criação e desenvolvimento, seja em sua assimilação no final da cadeia de consumo pelos cidadãos. Esta nova realidade de Internet das

Coisas, pautada pelo armazenamento, processamento e compartilhamento de dados, impõe uma discussão ética a ser feita a partir de um debate amplo entre diferentes atores, englobando empresas, governos e sociedade civil. Sem uma reflexão ética que norteie adequadamente a regulação jurídica, inclusive com relação à tutela da privacidade e dos dados pessoais, essa corre o risco de ser inócua ou nociva à coletividade.

Recentemente, o Parlamento Europeu editou uma resolução com recomendações da Comissão Europeia (2015/2103-INL)[726], propondo a criação de uma personalidade eletrônica para robôs inteligentes, entre outras propostas de regulamentação jurídica. Em sua justificativa, lê-se: "*Even if robots are not yet commonplace, the time has come to legislate*." Apesar de interessante a proposta, este tipo de regulação não pode ser precipitada, devendo passar amplamente pelas esferas deliberativas da sociedade. Defendemos, portanto, que o avanço jurídico-regulatório seja acompanhado de perto por um debate ético maduro e inclusivo nas esferas públicas das sociedades afetadas.

Por isso dedicaremos esse capítulo a tentar avançar nas discussões sobre ética aplicada a Coisas, incluindo nesta perspectiva - conforme defendido no primeiro capítulo deste trabalho -, as discussões sobre algoritmos e inteligência artificial, buscando compreender quais são seus efeitos democráticos hoje, pensando sob um ponto de vista regulatório.

3.1
O Embate entre Utilitarismo e Deontologia

Depois que a bomba explodiu, depois que ficou claro que os Estados Unidos poderiam arrasar uma cidade inteira com apenas uma bomba, um cientista virou-se para meu pai e disse: "Agora a ciência sabe o que é pecado". E sabe o que meu pai [cientista] falou? Ele disse: "O que é pecado?".

(Cama de Gato – Kurt Vonnegut, **1963**)

[726] Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-582.443+01+DOC+PDF+V0//PT&language=PT>. Acesso em: 27 set. 2017.

Quando se discute ética[727] e avanço tecnológico uma das discussões mais tradicionais que se costuma trazer *a priori* envolve o embate entre as visões contrastantes do utilitarismo / consequencialismo[728] e da deontologia, visto que a corrente adotada é determinante para a discussão de onde se pretende chegar e quais são as prioridades nessa análise. Nesse sentido, o caso concreto mais interessante para abordar esse primeiro tema ético, a título exemplificativo, é aquele envolvendo o carro Ford Pinto.

Entre os anos de 1971 e 1980, o Ford Pinto foi um modelo de automóvel produzido e vendido pela *Ford Motor Company*. Esse modelo, no entanto, teve problemas com incêndios do tanque de combustível associados com batidas na traseira do carro.

A falta de segurança do design do sistema de combustível do Ford Pinto levou a incidentes graves, resultando em processos judiciais, inclusive criminais, e muita controvérsia pública.[729] A controvérsia se deu em razão de a Ford ter sido acusada de saber que o carro possuía uma instalação de tanque insegura, mas ter

[727] Por conta de divergências corriqueiras, relacionadas ao sentido dos termos "ética" e "moral", não havendo um consenso em relação aos significados, vale dizer que ambas são frequentemente usadas como sinônimos, inclusive nesse trabalho. Alguns escritores distinguem os dois de maneiras que podem ser úteis para os teóricos legais. Por exemplo, podemos usar a palavra "ética" para se referir aos padrões normativos que se aplicam a alguns grupos específicos. Assim, podemos distinguir a "ética legal" ou "ética médica" das obrigações morais consideradas em todos os aspectos dos advogados e médicos. Contudo, por vezes, a "moralidade" é usada para se referir às normas morais de uma comunidade particular - em oposição à "ética" entendida como padrões normativos objetivamente corretos que têm aplicação universal. Outras vezes, esse sentido é invertido e a "ética" pode se referir aos padrões relativos à comunidade e a "moralidade" usada para padrões universais objetivamente válidos.

[728] Sobre a complexa distinção entre utilitarismo e consequencialismo, assim se posiciona o Stanford Encyclopedia of Philosophy: "*In actual usage, the term 'consequentialism' seems to be used as a family resemblance term to refer to any descendant of classic utilitarianism that remains close enough to its ancestor in the important respects. When such pluralist versions of consequentialism are not welfarist, some philosophers would not call them* utilitarian*. However, this usage is not uniform, since even non-welfarist views are sometimes called utilitarian. Whatever you call them, the important point is that consequentialism and the other elements of classical utilitarianism are compatible with many different theories about which things are good or valuable.*" Por não haver uma definição única para "consequencialismo" e por ele frequentemente ser compreendido como um tipo de "utilitarismo" ou apresentar aspectos fundamentais similares aos do utilitarismo, citaremos citaremos ambos de forma conjunta ou privilegiando o uso do conceito "utilitarista", com a conotação dada por Peter Singer: *The simplest form of consequentialism is classical Utilitarianism, which holds that every action is to be judged good or bad according to whether its consequences do more than any alternative action to increase—or, if that is impossible, to limit any unavoidable decrease in—the net balance of pleasure over pain in the universe. Disponível em: <https://www.utilitarian.net/singer/by/1985----.htm>. Acesso em: 20 set. 2017. Disponível em*: <https://plato.stanford.edu/entries/consequentialism/>. Acesso em: 20 set. 2017.

[729] The Center for Auto Safety. Ford Pinto Fuel Tank. Publicado em 13 Nov. 2009. Disponível em: <http://www.autosafety.org/ford-pinto-fuel-tank/>. Acesso em 19 Jun. 2017.

decidido por não fazer as alterações necessárias com base em uma análise de custo-benefício. *Grimshaw vs Ford* e *State of Indiana vs Ford Motor Company* são casos judiciais que resultaram de acidentes envolvendo este modelo de automóvel.[730]

A Ford realizou essa análise de custo-benefício em 1973, para submissão à National Highway Traffic Safety Administration (NHTSA), com intuito de fundamentar a objeção da Ford à proposta de uma regulação de sistema de combustível mais forte. A análise comparou o custo de reparos ao custo relacionado a lesões e mortes relacionadas com incêndios nos veículos vendidos nos Estados Unidos. No memorando, a Ford estimou o custo de modificações ao sistema de combustível para reduzir riscos de incêndio em $11 por veículo, aplicável a 12,5 milhões de carros e caminhões leves, chegando a um total de $137,5 milhões de custo para a empresa. Por outro lado, estimou-se que as mudanças no design evitariam 180 mortes por queimaduras e 180 lesões graves por ano, o que representava um custo de aproximadamente $49,5 milhões para a sociedade, de acordo com a tabela abaixo:[731]

A NHTSA iniciou a sua investigação sobre o modelo Ford Pinto em 1977, após a divulgação de artigos e manifestações que repudiavam a postura da empresa na fabricação do automóvel. Ao final do processo, a entidade indicou à Ford que fizesse o *recall* do carro. Para sofrer menos prejuízos relacionados à reputação da empresa, a esta realizou um *recall* voluntário, antes que a NHTSA lançasse a ordem formal de recall.[732]

O caso Ford Pinto traz à tona o debate acerca da ética de empresas em relação ao desenvolvimento de novos produtos e tecnologias. No caso americano, uma falha mecânica no desenho do projeto causou não apenas danos materiais, como também colocou em grave risco a vida e integridade física das pessoas. Além disso, mesmo tendo conhecimento sobre o potencial do dano, o produto continuou sendo comercializado por algum tempo pela empresa com base em uma visão econocêntrica, ainda que estivessem em risco vidas humanas. Defenderemos neste trabalho a importância de que o avanço tecnológico seja guiado por uma

[730] BINDER, Denis. *The Increasing Application of Criminal Law to Disasters and Tragedies*. Natural Resources & Environment, v. 30, n. 3, 2016.
[731] BAURA, Gail. *Engineering Ethics:* An Industrial Perspective. Cambridge: Academic Press, 2006. p. 39-50.
[732] ROSSOW, Mark P. *Ethics:* An Alternative Account of the Ford Pinto Case, 2015.

ética deontológica e não por uma visão utilitarista que sopese apenas as consequências.

A visão utilitarista clássica, preconizada por Jeremy Bentham em 1781[733], é caracterizada pelo que muitos autores chamam de consequencialismo. Deste modo, busca encontrar justificação nas consequências das ações, e não em máximas absolutas.[734] A visão utilitarista clássica[735] tem como um dos seus fundamentos o conceito de ato consequencialista que atrela o valor moral de toda ação a seus resultados, bons ou ruins, analisando a felicidade ou bem-estar geral que ela produz em uma perspectiva social.[736] Portanto, um ato é moralmente correto quando maximiza o bem, isto é, quando o valor total de bem gerado para todos menos a quantidade total de mau geral tiver um saldo líquido positivo. Ou seja, quando o resultado final da diminuição entre benefícios e malefícios for um bem geral.

Segundo o utilitarista Cláudio Costa: "[...] a ação moralmente correta é a que segue uma regra cuja adoção produz um bem maior para a sociedade que adota o sistema de regras à qual ela pertence".[737] Em suma, pode-se dizer que a máxima desta forma de pensar costuma ser retratada pela frase em inglês "*the greatest happiness for the greatest number*"[738]. Essa visão utilitarista clássica resiste, portanto, à ideia de que a justiça moral depende de qualquer outra coisa que não seja suas consequências.[739]

---

[733] BENTHAM, Jeremy. *Os pensadores*. São Paulo: Abril Cultural, 1979.
[734] Ibid.
[735] Rafael Zanatta explica a influência do pensamento utilitarista nas teorias de Richard Posner sobre law and economics: "Esta concepção utilitarista do ordenamento jurídico, fundada em princípios modernos individualistas, além de influenciar alguns economistas como David Ricardo, serviu de pressuposto moral para a estruturação lógico-racional das teorias jurídico-econômicas da Escola de Chicago, como constata Carlos Santiago Niño. Neste sentido, compreender o utilitarismo benthamiano é um pressuposto para a análise da teoria da eficiência da law and economics. É possível observar elementos centrais do pensamento utilitarismo benthamiano na análise econômica do direito (law and economics), corrente acadêmica norte-americana que tem como Richard Posner um dos seus principais expoentes e que será analisada num momento posterior. É a partir de Bentham que se pode compreender de que forma Richard Posner substitui o conceito de maximização das satisfações individuais (utilitarismo na forma clássica) pelo conceito de maximização da riqueza (eficientismo econômico) como critério de decidibilidade e avaliação do próprio sistema Judiciário." ZANATTA, Rafael. *O Utilitarismo de Jeremy Bentham*. 2010. Disponível em: <https://rafazanatta.blogspot.com.br/2010/04/o-utilitarismo-de-jeremy-bentham.html>. Disponível em: 20 set. 2017.
[736] MILL, John Stuart. *O utilitarismo.* São Paulo: Iluminuras, 2000.
[737] COSTA, C. Razões para o utilitarismo. *Ethic@*. Florianópolis: UFSC, v.1, n. 2, p. 155-174, 2002.
[738] Tradução livre do autor: A maior felicidade para o maior número de pessoas.
[739] SANCHEZ VASQUEZ, Adolfo. *Ética*. 14. ed. Rio de Janeiro: Civilizacao Brasileira, 1993.

Segundo John Rawls[740], um conjunto de problemas pode ser apontado no utilitarismo clássico do ponto de vista teórico e epistemológico. Em primeiro lugar, segundo Rawls, a teoria de justificação do utilitarismo está centrada na maximização do bem coletivo. Apesar de, a princípio, parecer positivo, Rawls atenta para o fato de haver o preterimento do direito que cada indivíduo possui em face do direito dito social, gerando situações injustas na medida em que a teoria não leva em consideração o modo de distribuição do bem geral entre cada cidadão individualmente compreendido.

Para ilustrar a tese acima sustentada, imagine a seguinte situação: cada um de cinco pacientes em um hospital morrerá sem um transplante de órgão. O paciente na sala 1 precisa de um coração, o paciente na sala 2 precisa de um fígado, o paciente na sala 3 precisa de um rim, e assim por diante. A pessoa no quarto 6 está no hospital para exames de rotina. Seu tecido é compatível com os outros cinco pacientes, e um especialista está disponível para transplantar seus órgãos para os outros cinco. Esta operação salvaria suas vidas, enquanto que mataria o "doador". Não há outra maneira de salvar nenhum dos outros cinco pacientes. Sob a ótica consequencialista, parece que matar o "doador" vai maximizar o bem-estar geral, uma vez que cinco vidas têm mais utilidade para a sociedade do que apenas uma. Se assim for, então tal teoria implica que não seria moralmente errado para o médico realizar o transplante, mas pelo contrário, que esta seria a medida correta a se adotar.[741]

A partir desse exemplo, percebemos uma perspectiva temerária para a sociedade quando há a desconsideração do direito individual como legítimo – como, por exemplo, o direito à vida que detém o doador. Nesse sentido, afirmou Rawls sobre o utilitarismo: "*o bem (the good) é definido independentemente do justo (the right), e então o justo (the right) é definido como aquilo que maximiza o bem (the good)"*. Isto é, de acordo com o autor, tal teoria caracteriza a maximização da felicidade como aquilo que é moralmente bom sem se atentar para o que é justo e isso, no fim das contas, tem um impacto direto negativo na sociedade. Em suas palavras: [742]

[740] RAWLS, John. *A Theory of Justice*. Harvard, 1971.
[741] SANDEL, Michael. Justiça. *O que é fazer a coisa certa?*. Civilização Brasileira. Rio de janeiro, 2009.
[742] RAWLS, John. *A Theory of Justice*. op.cit.

> Nessa concepção da sociedade os indivíduos isolados são vistos como um número correspondente de linhas ao longo das quais direitos e deveres devem ser atribuídos e os parcos meios de satisfação distribuídos de acordo com certas regras, de modo a permitir o preenchimento máximo de carências. A natureza da decisão tomada pelo legislador ideal não é, portanto, substancialmente diferente da de um empreendedor que decide como maximizar seus lucros por meio da produção desta ou daquela mercadoria, ou da de um consumidor que decide como maximizar sua satisfação mediante a compra desta ou daquele conjunto de bens. Em cada um desses casos há uma única pessoa cujo sistema de desejos determina a melhor distribuição de meios limitados. A decisão correta é essencialmente uma questão de administração eficiente. Essa visão da cooperação social é a conseqüência de se estender à sociedade o princípio da escolha para um único ser humano, e depois, fazer a extensão funcionar, juntando todas as pessoas numa só através dos atos criativos do observador solidário e imparcial. O utilitarismo não leva a sério a diferença entre as pessoas.[743]

No mesmo sentido, segundo o professor de Harvard Michael Sandel[744], a maioria das pessoas acha esse tipo de resultado abominável moralmente, assim como consideram reprovável a fundamentação utilitária e econômica da Ford para tentar justificar a decisão empresarial de manter seu carro defeituoso sendo comercializado no mercado.[745]

Em segundo lugar, finalmente, o utilitarismo clássico parece exigir que os agentes calculem todas as consequências que seus atos terão no futuro. Entretanto, isso é, via de regra, impossível, sobretudo na área tecnológica. Muitos utilitaristas clássicos, como Stuart Mills[746] e Posner[747], não propõem seus princípios como meros procedimentos de decisão, mas como um padrão do que seria moralmente correto. Assim, suas teorias têm a intenção de definir as condições necessárias e suficientes para que um ato maximize valores morais e, consequentemente, o

[743] RAWLS, John. *Uma teoria da justiça*. Trad. Almiro Pisetta e Lenita Maria Rimoli Esteves. 2. ed. São Paulo: Martins Fontes, 2002, p. 25.
[744] SANDEL, Michael. *Justiça.* O que é fazer a coisa certa?. Civilização Brasileira. Rio de janeiro, 2009.
[745] O dilema do bonde é outro clássico exercício de pensamento em ética, idealizado por Philippa Foot e analisado por Judith Jarvis Thomson, para contrastar a visão utilitária - consequencialista com a perspectiva deontológica. A situação idealizada é a seguinte: um bonde está fora de controle em uma estrada. Em seu caminho, cinco pessoas amarradas na pista. Entretanto, é possível apertar um botão que encaminhará o bonde para um percurso diferente, mas ali, por desgraça, se encontra outra pessoa também atada. Deveria apertar-se o botão? A partir da corrente consequencialista, deveria ser apertado o botão. Pode-se concluir isto a partir da máxima do ato consequencialista, segundo a qual um ato é moralmente correto se, e somente se, esse ato maximiza o bem, isto é, se o valor total de bem para todos menos a quantidade total de maus para todos possui um saldo líquido positivo para o bem geral. Tendo em vista no caso em questão que 5 pessoas seriam salvas, mesmo às custas da morte de 1 pessoa, o resultado final seria um bem maior.
[746] MILL, John Stuart. *O utilitarismo.* São Paulo: Iluminuras, 2000. Tradução de: The utilitarism.
[747] POSNER, Richard. *Economic Analysis of Law*. Chicago, 2014.

bem-estar da sociedade, independentemente de o agente saber antecipadamente se essas condições serão – ou não - cumpridas.[748][749]

Esse problema se intensifica no cenário de Internet das Coisas, que traz mais imprevisibilidade para a equação e torna ainda mais difícil, quiça inviável, qualquer tomada de decisão que se dê em função apenas do resultado ou da consequência. Nesse contexto, se valer de cálculos exatos para maximização de um bem futuro pode levar a frustrações e a resultados muito insatisfatórios, como se verá adiante, em função de variáveis não ponderáveis em um momento anterior.[750]

Em contraposição ao pensamento utilitarista, a teoria deontológica possui seu foco na ação do agente e não em suas consequências. Segundo esta perspectiva, escolhas consequencialistas menosprezam direitos individuais e, desta forma, mensuram quais vidas ou "*felicidades*" valem mais – o que não deve ser feito, visto que cada indivíduo deve ser considerado como um fim em si mesmo.[751]

A deontologia enquadra-se no domínio das teorias morais que orientam e avaliam o que devemos fazer e de modo diverso das teorias utilitaristas, essas julgam a moralidade das escolhas individualmente, por um parâmetro não orientado pelos resultados.[752]

O primeiro grande filósofo a definir princípios deontológicos foi Immanuel Kant[753], fundador alemão da filosofia crítica do século XVIII e talvez o

[748] FRANKENA, Willian K. *Etica*. Rio de Janeiro : Zahar, 1969. 143p.
[749] Disponível em: <https://plato.stanford.edu/entries/consequentialism/#WhaGooHedVsPluCon>. Acesso em: 10/01/2018.
[750] Disponível em: <https://plato.stanford.edu/entries/consequentialism/#WhaGooHedVsPluCon>. Acesso em: 10/01/2018.
[751] Disponível em: <https://pt.wikipedia.org/wiki/Dilema_do_bonde>. Acesso em: 29 abr. 2017.
[752] Disponível em: <https://plato.stanford.edu/entries/ethics-deontological/#AgeCenDeoThe>. Acesso em: 29 abr. 2017.
[753] A teoria da ética de Immanuel Kant pode ser considerada deontológica primeiramente pelo fato de Kant argumentar que, para agir de maneira moralmente correta, as pessoas devem agir conforme o dever (deon). Em segundo lugar, para Kant, não são as conseqüências das ações que as tornam corretas ou erradas, mas os motivos da pessoa que realiza a ação. "*Kant then argues that the consequences of an act of willing cannot be used to determine that the person has a good will; good consequences could arise by accident from an action that was motivated by a desire to cause harm to an innocent person, and bad consequences could arise from an action that was well-motivated. Instead, he claims, a person has a good will when he 'acts out of respect for the moral law'. People 'act out of respect for the moral law' when they act in some way because they have a duty to do so. So, the only thing that is truly good in itself is a good will, and a good will is only good when the willer chooses to do something because it is that person's duty, i.e. out of "respect" for the law." Kant, Immanuel. 1785. First Section: Transition from the Common Rational*

maior representante dos ideais iluministas.[754] Kant preconizava o lema "*atrever-se a conhecer*" e em um ensaio datado de 1784, *Was ist Aufklärung?* (O que é o Iluminismo?), sugere que o movimento iluminista representa a evasão dos homens do estado de *minoridade*, conceito que para Kant significa incapacidade de servir-se do próprio intelecto.[755] Nas palavras do próprio filósofo:

> "O iluminismo representa a saída dos seres humanos de uma tutelagem que estes mesmos impuseram a si. Tutelados são aqueles que se encontram incapazes de fazer uso da própria razão independentemente da direção de outrem. É culpado da própria tutelagem quando esta resulta não de uma deficiência do entendimento, mas da falta de resolução e coragem para se fazer uso do entendimento independentemente da direção de outrem. *Sapere aude*! ("atreva-se a conhecer") Tem coragem para fazer uso da tua própria razão!"[756]

Segundo Fraga:

> "o movimento iluminista inspirou uma visão de mundo que ajudou a gerar acontecimentos e eventos importantes como os já citados acima, além de outros tantos em menor escala. Mais do que isso, os ideais do iluminismo embalaram uma cosmovisão que atravessou os séculos XIX e XX, e que estava composta por elementos como a confiança na razão, a fé no progresso moral do ser humano, o crédito para o avanço do humanismo universalista. Como exemplo disso pode-se fazer alusão à Declaração Universal dos Direitos do Homem promulgada pela ONU em 1948, cuja evidente inspiração é a declaração de direitos do homem da Revolução Francesa, e onde foram reafirmados ideais como a liberdade e igualdade de todos os homens."[757]

De acordo com Kant, uma boa vontade é aquela que quer agir de acordo com a lei moral, por respeito a essa lei, e não por inclinações naturais.[758] Ele viu a

---

Knowledge of Morals to the Philosophical, Groundwork of the Metaphysic of Morals. Kant, Immanuel (1785). Thomas Kingsmill Abbott, ed. Fundamental Principles of the Metaphysic of Morals (10 ed.). https://en.wikipedia.org/wiki/Deontological_ethics#cite_note-transition-11.

754 Segundo Fraga: O Iluminismo pode ser definido como um movimento filosófico surgido ao longo do século XVIII que se caracterizou pela confiança no progresso e na razão, pelo desafio à tradição e à autoridade e pelo incentivo à liberdade de pensamento. À idéia de progresso técnico estava associada uma crença no progresso moral da humanidade. Um expressivo compromisso do movimento Iluminista é o de melhoria da vida individual e coletiva do ser humano. Vide: https://esbocosfilosoficos.com/2014/03/14/a-visao-politica-de-thomas-hobbes/.

[755] Kant, Immanuel (1784). Beantwortung der Frage : Was ist Aufklärung.

[756] Ibid.

[757] Disponível em: <https://esbocosfilosoficos.com/2014/03/14/a-visao-politica-de-thomas-hobbes/>. Acesso em: 29 abr. 2017.

[758] Nas palavras de Orlando Brunet: "Kant considerava a distinção entre o certo e o errado uma questão real e palpável. Para ele todas as pessoas sabem distinguir uma coisa da outra não por ter aprendido, mas porque todos possuímos uma razão prática que nos diz em qualquer tempo o que é certo e errado em nossa esfera moral – essa capacidade, que é a lei moral é tão absoluta quanto as leis da física. Ela antecede toda e qualquer experiência e não se vincula a nada que envolva uma escolha, pois é imperativa, absoluta e abrangente. Para Kant a lei moral é a consciência humana, que nos distingue dos animais, não pode ser comprovada pela razão, mas é inevitável. Quando faço algo, tenho que me certificar que qualquer um faria o mesmo naquela situação. Nisso implica

lei moral como um imperativo categórico e acreditava que seu conteúdo poderia ser estabelecido através da racionalidade humana. Kant enuncia o imperativo categórico com três diferentes formulações (e suas variantes). São estas:[759]

> (i) Lei Universal: "Age como se a máxima de tua ação devesse tornar-se, através da tua vontade, uma lei universal." Variante: "Age como se a máxima da tua ação fosse para ser transformada, através da tua vontade, em uma lei universal da natureza."
> (ii) Fim em si mesmo: "Age de tal forma que uses a humanidade, tanto na tua pessoa, como na pessoa de qualquer outro, sempre e ao mesmo tempo como fim e nunca simplesmente como meio."
> (iii) Legislador Universal (ou da Autonomia): "Age de tal maneira que tua vontade possa encarar a si mesma, ao mesmo tempo, como um legislador universal através de suas máximas." Variante: "Age como se fosses, através de suas máximas, sempre um membro legislador no reino universal dos fins."

As formas mais conhecidas de deontologia, e também as formas que apresentam maior contraste com o utilitarismo, sustentam que algumas escolhas não podem ser justificadas por seus efeitos – como elucidado acima. Em tais relatos deontológicos sobre a moralidade, os agentes não podem fazer certas escolhas erradas, ainda que as consequências fossem nobres. Para os deontologistas, o que torna uma escolha certa é a sua conformidade com o dever moral, que deve ser obedecido por cada agente da sociedade, indendepentemente do sopesamento das consequências.[760] As restrições deontológicas podem ser entendidas como derivadas da própria virtude da racionalidade.

Outra característica significativa das teorias éticas deontológicas é que estas tratam de moralidades relativas a agentes. A relatividade do agente nas teorias deontológicas se contrapõe a sua neutralidade na teoria utilitarista clássica. Como esclarecido acima, esta última defende uma teoria moral neutra do agente considerando a felicidade geral como o único fator que precisa ser pesado na determinação do que se deve fazer. A identidade e os interesses do ator devem ser desconsiderados na hora de se julgar uma ação. Já as teorias morais deontológicas

---

seu imperativo categórico, que demanda que devemos tratar o outro com um fim em si mesmo, e não como um meio. Não posso usar outros ou a mim mesmo como meio – por isso a ética de Kant é descrita como a ética do dever. Para o filósofo, somente quando em consonância com a lei moral é que sou verdadeiramente livre, pois quando escravos da causalidade não temos livre arbítrio – vide os animais. Porém, quando nos submetemos a lei moral, somos nós que determinamos a lei que vai nos governar." Vide: https://faceaovento.com/2015/07/03/a-lei-moral-e-o-imperativo-categorico-de-kant/.

[759] KANT, Immanuel. *Fundamentação da Metafísica dos Costumes* (Grundlegung zur Metaphysik der Sitten, 1785). Trad: Paulo Quintela: Edições 70, 2008.

[760] Disponível em: <https://plato.stanford.edu/entries/ethics-deontological/#AgeCenDeoThe>. Acesso em: 29 abr. 2017.

reconhecem a importância da existência de obrigações especiais, e aqui, a identidade do agente faz uma diferença crucial para a decisão do que se deve fazer.

Em outras palavras, de acordo com o utilitarismo clássico, a ação correta é aquela que traz as melhores consequências. O fato de que alguém prometeu fazer algo é vinculativo somente na medida em que é a ação que maximiza a utilidade. De maneira oposta, um deontólogo achará isso contra-intuitivo e argumentará que o fato de alguém ter prometido algo faz a diferença para saber se uma ação é correta ou errada, independentemente do valor das conseqüências decorrentes do cumprimento da promessa. Isso ocorre porque (alguns) deveres são relativos ao agente e dependem de fatos sobre o contexto e o histórico do agente.[761]

Além disso, os utilitaristas sentem-se em posição de determinar quais ações aumentam o bem sendo, portanto, moralmente justificáveis. No entanto, não há uma definição universal do que seria esse "bem" - até mesmo os adeptos dessa teoria diferem amplamente em termos de especificação do bem[762]. Portanto, parte do problema da utilização desta tese decorre da vagueza do conceito de utilidade e a ausência de critérios de mensurabilidade de felicidade.

Esses são alguns dos motivos que nos levam a crer que, para fins de orientar os avanços tecnológicos, a corrente utilitária não deve ser considerada adequada para uma aplicação isolada. Deve ser levada em consideração, mas sempre restrita à perspectiva deontológica.[763]

Há, ainda, um outro ponto crucial, ora abordado de maneira breve: quando pensamos em novas tecnologias, envolvendo novas capacidades de agência como autoprogramação, *machine learning*[764] e *deep learning*[765], nos deparamos com invenções que não permitem, muitas vezes, a previsão de consequências.

---

[761] Disponível em: <http://www.newworldencyclopedia.org/entry/Deontological_ethics>. Acesso em: 29 abr. 2017.

[762] Tradução livre do autor.

[763] Há teóricos que defendem a aplicação conjunta do consequencialismo com a deontologia, originando a chamada "teoria mista". Vide: https://plato.stanford.edu/entries/ethics-deontological/#DeoRelConRec.

[764] Os sistemas AI precisam da capacidade de adquirir seus próprios conhecimentos, extraindo padrões de dados brutos. Esta capacidade é conhecida como aprendizado automático. O aprendizado de máquinas permitiu que os computadores abordassem problemas envolvendo conhecimento do mundo real e tomassem decisões que pareciam subjetivas.

[765] O termo moderno "Deep Learning" vai além da perspectiva neurocientífica sobre a atual geração de modelos de aprendizagem de máquinas. Apela a um princípio mais geral de aprendizagem de múltiplos níveis de composição, que podem ser aplicados em estruturas de

Conforme nos ensina o pesquisador holandês Peter Kroes, ainda que um designer possa antecipar diferentes conseqüências não planejadas e não determinadas, ele não pode evitar que todas essas conseqüências negativas surjam. A partir desse ponto de vista, o desenvolvimento tecnológico sempre tem um caráter experimental: algumas conseqüências sociais de uma determinada tecnologia só emergem quando esta é implementada.[766]

O cenário de Internet das Coisas e o avanço da Inteligência Artificial traz à tona agentes capazes de agir de forma semelhante a humanos, inclusive no que tange a comportamentos menos previsíveis. Mais do que simples ferramentas que exercem funções pré-estabelecidas, estes podem desenvolver uma forma própria de agir, produzindo impactos no mundo de forma cada vez menos determinável ou controlável por agentes humanos. Quanto mais adaptáveis se tornam os programas de inteligência artificial, mais imprevisíveis passam a ser suas ações.

Segundo Kroes:[767]

> Isto se dá, em parte, também ao fato de que a sociedade geralmente muda quando essa tecnologia está incorporada; tecnologia e sociedade se desenvolvem conjuntamente à medida que se expressam. (...) Consequências não intencionais não podem ser totalmente previstas ou, de fato, evitadas. Isso não é apenas algo causado por nossa limitada capacidade de conhecimento, mas também pelo fato de que consequências não desejadas são, muitas vezes, o resultado das ações de múltiplos atores dentro de um sistema sociotécnico. A implicação disto é que o desenvolvimento responsável da tecnologia é mais complicado do que se presumiu. (...) Engenheiros podem antecipar a ocorrência de efeitos não intencionais, esforçando-se para criar projetos robustos, flexíveis e transparentes. A natureza experimental da tecnologia, finalmente, dá origem à questões éticas das condições sobre as quais essas experiências seriam moralmente aceitáveis.[768]

---

aprendizagem de máquinas que não são necessariamente inspiradas nos sistemas neurais humanos.

[766] KROES, Peter. et al. *A Philosophy of Technology* From Technical Artefacts to Sociotechnical [s.l.]: Systems. Morgan & Claypool Publishers, 2011.

[767] Ibid.

[768] Tradução livre do autor. No original: *This is partly down to the fact that society also often changes when that technology is embedded; technology and society codevelop as it is phrased.* (…) *Unintended consequences cannot be entirely predicted or, for that matter, avoided. This is not just something that is caused by our limited knowledge capacity but also by the fact that the unintended consequences are often the result of the actions of many actors within a sociotechnical system. The implications of this observation are that responsibly developing technology is more complicated than was presumed. (...) Engineers can anticipate the occurrence of unintended effects by endeavouring to come up with designs that are robust, flexible and transparent. The experimental nature of technology, finally, gives rise to the ethical question of the conditions under which such experiments are morally acceptable.*

Com o avanço das novas tecnologias, a preocupação envolvendo a escolha em seguir determinações deontológicas ou utilitaristas e econocêntricas se torna ainda mais importante. Isso porque, enquanto em casos como o Ford Pinto, por exemplo, o defeito encontrado no modelo de automóvel poderia ser detectado e corrigido, muitas vezes os efeitos de uma inovação tecnológica podem ser quase impossíveis de prever. Além disso, o risco pode ser agravado ou prolongado por uma visão comercial utilitarista, trazendo maiores prejuízos a seres humanos.[769]

A inteligência artificial, especialmente, merece destaque nessa discussão, porque trata justamente da tentativa de se criarem mecanismos capazes de "pensar" de forma relativamente autônoma. Portanto, não se recomenda a adoção da perspectiva utilitarista para pensar os desafios da hiperconectividade.

Corroborando com esta visão, a ênfase internacional hoje na proteção dos direitos humanos - e, portanto, no dever de não violá-los - pode ser vista como uma prevalência da perspectiva deontológica, especialmente relacionada à proibição de se usar uma pessoa como um meio e não como um fim em si mesma.[770] Em complemento, o eticista Hans Jonas ao pensar sobre a ética adequada à civilização tecnológica, chama atenção para a necessidade de atualização do imperativo categórico kantiano para: aja de modo que os efeitos da sua ação não sejam destrutivos para a possibilidade futura de vida humana na Terra ou de maneira mais simples; não ponha em perigo as condições necessárias para a conservação indefinida da humanidade sobre a Terra. A releitura do imperativo realizada por Jonas reforça o fato de que na era digital nós não temos o

[769] Mencionamos no capítulo anterior desse trabalho o conceito de "riscos do desenvolvimento" que podem ser entendidos como aqueles que só vêm a ser descobertos pelo fabricante após um período de uso do produto. Levou-se em consideração o fato de que o fabricante é o agente que tem as melhores condições de prever os efeitos negativos e ponderar sobre as consequências do uso de um produto antes de colocá-lo no mercado. Além disso, reforçamos o argumento do chamado "risco do negócio", encampado pelo atual CDC nos arts 12 e 14, criando uma responsabilidade civil objetiva. Os fabricantes lucram com a atividade e os produtos e, por consequência, deveriam estar mais preparados para suportar os prejuízos decorrentes dos danos que os seus produtos possam causar à sociedade, seja sob o âmbito da contratação de seguros para indenização seja pela distribuição do prejuízo no custo do produto. Esse raciocínio pode servir como um incentivo na preocupação constante de o fabricante somente colocar em circulação produtos que sejam seguros. TULA, Wesendonck. A responsabilidade civil pelos riscos do desenvolvimento: evolução histórica e disciplina no Direito Comparado. Direito & Justiça v. 38, n. 2, p. 213-227, jul./dez. 2012. CALIXTO, Marcelo Junqueira. O art. 931 do Código Civil de 2002 e os riscos do desenvolvimento. *Revista Trimestral de Direito Civil*, Rio de Janeiro, Padma v. 6, n. 21, p. 75-77, jan./mar. 2005. SILVA, João Calvão da. *A responsabilidade civil do produtor*, p. 75.

[770] Disponível em: <https://www.britannica.com/topic/deontological-ethics>. Acesso em: 29 abr. 2017.

direito de escolher a não-existência de futuras gerações em função da existência da atual, ou mesmo de as colocar em risco.[771]

A importância destas questões está em termos maior clareza e pensarmos sobre o tipo de ética que deve nortear os avanços tecnológicos, bem como que tipo de responsabilidades devemos atribuir a agentes humanos e não-humanos neste contexto, tendo em vista seu potencial impacto na sociedade.

Para isso, exploraremos a partir de agora os efeitos de determinadas inovações tecnológicas na esfera pública, em sua concepção idealizada pelo filósofo alemão Jürgen Habermas, influenciado pelo pensamento deontológico kantiano supramencionado.[772]

Habermas abordou o tema da modernidade de forma otimista, com forte crença no desenvolvimento da razão e na crescente emancipação humana. O teórico propôs a substituição do chamado racionalismo instrumental pelo racionalismo comunicativo, que é expresso por meio do discurso.

Segundo Habermas, na medida em que a razão se torna instrumental[773], a ciência vai deixando de ser uma forma de acesso aos conhecimentos verdadeiros para tornar-se um instrumento de dominação, poder e exploração, sendo sustentada por uma ideologia contrária ao espírito iluminista e à emancipação da Humanidade, reforçada pelos meios de comunicação de massa.[774]

As questões de esfera pública de Habermas estão ligadas à evolução tecno-social e à concepção kantiana de uso público da razão[775], entendida como um fator essencial para se atingir o processo de esclarecimento - "*Aufklärung*". Esse processo, para Habermas, conforme veremos, depende da ação comunicativa na

[771] JONAS, Hans. O princípio da responsabilidade: ensaio de uma ética para a civilização tecnológica. Ed. Contraponto. Rio de Janeiro. 2015.

[772] Apesar de poder ser considerado herdeiro da tradição deontológica de Kant, Habermas, no entanto, vai além de uma ética puramente deontológica ao propor uma ética mais procedimentalista. A ética habermasiana permite considerar alguns aspectos da realidade, menos abstratos, como os parâmetros das condições ideias de fala e permite o fortalecimento do poder decisório e deliberativo dos cidadãos com base na razão.

[773] Razão instrumental é um termo usado pelos teóricos da Escola de Frankfurt para designar o estado em que os processos racionais são plenamente operacionalizados e atrelados à ideia de que conhecer é dominar e controlar a natureza e os seres humanos.

[774] HABERMAS, J. Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy, Cambridge, Polity Press, 1992.

[775] KANT, I. A Paz Perpétua e Outros Opúsculos, Lisboa, Edições 70, 1784 (1992). Habermas, J. The Theory of Communicative Action: Reason and the Rationalization of Society, (vol. 2), Cambridge: Polity Press, 1986.

esfera pública, refletido a partir do debate racional-dialógico capaz de atingir o consenso e o verdadeiro conhecimento.[776]

Partindo de uma ótica regulatória e deontológica, o contraste entre a teoria de Habermas e os avanços tecnológicos relacionados ao cenário de Internet das Coisas, nos ajudará a pensar o quanto estamos nos distanciando de um contexto democraticamente positivo envolvendo determinadas tecnologias e regulações. Ao final do capítulo pretendemos complementar a lente deontológica habermasiana para se pensar a dinâmica da esfera pública na era da hiperconectividade, razão pela qual proporemos novas sobreposições teóricas.

3.2
A Esfera Pública Colonizada por Algoritmos: Artefatos Não-Humanos na Esfera Pública Conectada

Conforme vimos no item anterior, é importante que busquemos, para os propósitos de regulação da IoT, a prevalência da perspectiva deontológica. Este primeiro alicerce nos permite contornar os abusos advindos da perspetiva utilitarista, impedindo que se use uma pessoa como um meio e não como um fim em si mesma, possibilitando pensarmos nos deveres e na eticidade atrelados às diferentes ações e procedimentos intrinsecamente, independentemente das consequências.[777] A partir disso, podemos pensar então qual a perspectiva ética mais adequada para atender deontologicamente aos procedimentos e ações democráticas relacionadas ao complexo mundo de dados e de constante interação homem-máquina (Coisa) em que vivemos.

Com esse propósito, entende-se que a perspectiva teórica de Jürgen Habermas deve ser levada em consideração. A justificativa para isso está na completude e complexidade da teoria habermasiana, que nos permite pensar sobre o avanço deste novo mundo de dados de maneira dialógica e participativa para atingir proposições regulatórias mais legítimas e consensuais.[778]

---

[776] HABERMAS, J. Between *Facts and Norms:* Contributions to a Discourse Theory of Law and Democracy, Cambridge, Polity Press, 1992.

[777] Impõe-se, portanto, um 'dever ser' ético e moral não somente atrelado às finalidades, mas também a todo o procedimento e gama de ações.

[778] Os principais conceitos e formulações do pensador Jürgen Habermas e sua relação com as plataformas de Internet foram profundamente descritos em trabalho anterior do autor desta tese (na

O pensador alemão Jürgen Habermas, nascido em 1929, vivenciou na Alemanha pós-guerra, com os julgamentos de Nuremberg, a profundidade do fracasso moral e político da Alemanha no âmbito do nacional-socialismo.[779] Habermas destacou-se no mundo acadêmico ao analisar o desenvolvimento da esfera pública burguesa desde as origens, nos salões do século 18, até a sua transformação através da influência de meios de comunicação dirigidos pelo capital.[780]

Para Habermas, a legitimidade das normas e do sistema político em sociedades ocidentais capitalistas contemporâneas, depende da aceitação das normas pelos cidadãos. Isso ocorre por meio de sucessivas tentativas de justificação nas quais cada cidadão deve vincular livremente sua vontade ao conteúdo da norma através de um processo racional e dialógico de argumentação, isto é, de reflexão e convencimento.

Neste tipo de sociedade, a esfera pública é entendida justamente como o conjunto de espaços que permitem a ocorrência dos processos dialógicos comunicacionais de articulação de opiniões e de reconstruções reflexivas dos valores, disposições morais e normativas que orientam a convivência social. É na esfera pública que os diferentes grupos constitutivos de uma sociedade múltipla e diversa partilham argumentos, formulam consensos e constroem problemas e soluções comuns.[781]

Conforme explicado previamente em trabalho do autor desta tese[782], a esfera pública de Habermas constitui uma zona de intercâmbio[783] entre o sistema, de um lado, e os setores privados do mundo da vida de outro. O sistema é

---

obra "Democracia Conectada"), razão pela qual não nos aprofundaremos tanto nos conceitos básicos do autor ou justificaremos exaustivamente sua ligação com as esferas digitais.

[779] Disponível em: <https://plato.stanford.edu/entries/habermas/>. Acesso em: 28 nov. 2017.

[780] Com a publicação em 1962 de sua habilitação, Strukturwandel der Öffentlichkeit (Transformação Estrutural da Esfera Pública, ed. Inglesa, 1989).

[781] MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.

[782] Ibid.

[783] "Além disso, compreendendo o intercâmbio de influências que ocorre entre mundo da vida e sistema sediado na esfera pública, ocorre nesta o embate entre as lógicas inerentes aos dois espaços. Referimo-nos ao embate entre agir comunicativo e agir racional. O primeiro é orientado para o entendimento intersubjetivo no qual os participantes buscam o consenso em torno de referências aos mundos objetivo, social e subjetivo. O segundo orienta-se na busca pelo êxito, distinguindo-se entre ação instrumental e ação estratégica." MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.

caracterizado por Habermas como o mundo do trabalho, pautado pela lógica do dinheiro e do poder[784], como um mundo instrumental de ação estratégica, e não comunicativa, orientado pelo mercado e pela burocracia[785]. O mundo da vida, por sua vez, é descrito por Habermas como o mundo da interação privada, que se organiza comunicativamente através da língua ordinária viabilizando a ação comunicativa sem um agir estratégico, orientada somente para o entendimento intersubjetivo que conduz idealmente ao acordo ou leva ao consenso.[786]

Ao analisar a transformação da esfera pública burguesa dirigida pelo poder do capital por meio da influência de meios de comunicação, Habermas alerta para a forte tendência à "colonização do mundo da vida" pelo sistema e seus valores. A colonização decorre, para o autor, da intromissão da política e economia no mundo da vida, responsável pela redução da cidadania e transformação dos cidadãos em clientes dos serviços de bem-estar social, sendo esta, segundo Habermas, a marca da modernidade. Neste cenário, o poder do capital econômico e da política invadem destrutivamente o mundo da vida. Segundo o teórico, a intervenção sistêmica intervém destrutivamente na reprodução cultural, na integração social e na socialização, como componentes do mundo da vida.[787]

Embora Habermas não tenha se debruçado específica e deliberadamente sobre o tema da Internet, em esforço intelectual a partir da categorização do autor, defendeu-se na obra **Democracia Conectada** [788], a possibilidade de se compreender as plataformas digitais como esferas públicas abstratas, dotadas de grande potencial comunicativo e democrático. Encontramos nos espaços digitais conectados uma esfera pública na qual indivíduos se comunicam regularmente, através de fóruns de discussão, redes sociais, ou plataformas de troca de

---

[784] Sistema econômico e poder político administrativo.

[785] HABERMAS, Jürgen. *The Theory of Communicative Action*. Beacon Press. 1987. v. II, p. 113-197 e CALHOUN, Craig (ed.). *Habermas and the Public Sphere*. The MIT Press, 1992. p. 1-51.

[786] "As esferas públicas são o lugar por excelência para a deliberação política e autodeterminação democrática. O sistema político, entendido como o aparato burocrático do Estado, cede lugar para que as deliberações políticas ocorram nas esferas públicas, visando a formação coletiva da vontade, a justificação de decisões previamente acertadas e o surgimento de novas identidades. E através dos procedimentos democráticos e das suas pressuposições comunicativas, a soberania popular é reinterpretada intersubjetivamente." MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014. p. 25.

[787] Apesar de Habermas prever que não haja uma blindagem completa do mundo da vida da lógica sistêmica, acredita na capacidade dessa lógica ser anulada pela própria dinâmica do mundo da vida, pautado no agir comunicativo.

[788] MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014. p. 25.

mensagens, que se aproximam muito da concepção de esfera pública desenhada por Habermas em menor escala.

> A Internet apesar de não ter sido caracterizada ou até mesmo estudada como uma esfera pública, faz-se necessário o esforço de inclui-la nesse conceito. As plataformas digitais são usadas hoje pela sociedade, inclusive a brasileira, de forma geral para o compartilhamento de informações e para promoverem, especificamente, um maior grau de participação e engajamento em questões de interesse público. As tecnologias da maneira como estão sendo utilizadas têm transformado indivíduos em uma importante fonte de informação, engajamento sociopolítico e controle do poder público, permitindo um maior de empoderamento dos cidadãos para desencadearem processos de transformação social e ao mesmo tempo uma maior legitimidade do poder político. Todos esses fatores são representativos da emergência de uma esfera pública conectada e com potencial democrático significativo ainda a ser explorado e mensurado.[789]
> (...)
> Observa-se, em primeiro lugar, que a tecnologia digital, combinada com a infraestrutura da Internet, se distingue de maneira substantiva das tradicionais mídias. Trata-se de uma plataforma de comunicação de duas vias, através da qual participantes não são meros receptores passivos de conteúdo. A importância dessas ferramentas digitais é possibilitar a criação de um novo ambiente comunicativo, que permite a qualquer um, a um preço muito mais acessível do que no passado recente, transmitir suas ideias com uma facilidade sem precedentes.
> (...)
> Os novos ambientes digitais representariam, portanto, ao menos potencialmente tendo por base estas características, uma multiplicação de esferas públicas, ampliando quantitativamente e qualitativamente os espaços disponíveis para o debate racional dialógico.[790]

No entanto, com o avanço das tecnologias digitais mais recentes, acompanhamos a transformação também desses espaços conectados, sendo possível vislumbrar uma possível redução no seu potencial comunicativo democrático.

Conforme descrito no capítulo anterior, observamos hoje a predominância nas esferas conectadas dos lucrativos modelos de negócio baseados em filtragem algorítmica com a finalidade de realizar práticas de *micro-targeting*, *profiling*, entre outras, mencionadas, direcionando a venda de produtos e serviços de forma otimizada a *e*-consumidores. Essas práticas correntes, conforme vimos, pautam-se pela utilização em grande medida dos dados pessoais dos usuários e geram o agravamento do efeito denominado "*filter bubble*", possuindo efeitos

[789] MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.

[790] Ibid.

democráticos nocivos e freiando o entusiasmo acerca do papel democrático da Internet como esfera pública para as sociedades contemporâneas.[791]

A *Filter Bubble* (ou filtros-bolha) pode ser definida como um conjunto de dados gerado por todos os mecanismos algorítmicos, utilizados para se fazer uma edição invisível voltada à customização da navegação *on-line*. Em outras palavras, é uma espécie de personificação dos conteúdos da rede, feita por determinadas empresas como o *Google*, através de seus mecanismos de busca, e redes sociais como o *Facebook*, entre diversas outras plataformas e provedores. Forma-se então, a partir das características de navegação de cada pessoa, um universo particular *on-line,* condicionando sua navegação. Isto se dá por meio do rastreamento de diversas informações, dentre elas, a localização do usuário e o registro dos *cookies*[792] - dados de acesso que consistem nas "pegadas digitais" deixadas ao se transitar e se manifestar pelos ambientes *on-line*.

Na linha de como os mecanismos de navegação estão se configurando, a Internet estaria se transformando em um espaço no qual é mostrado o que se acha que é de nosso interesse. Assim, quase sempre nos é ocultado aquilo que de fato desejamos ou eventualmente precisamos ver. Desse modo, pode-se dizer que a *filter bubble* pode implicar em restrições a direitos fundamentais como acesso à informação, liberdade de expressão, bem como à própria autonomia dos indivíduos, sendo prejudicial de forma geral, podemos dizer, para o debate e a formação de consenso na esfera pública conectada.

[791] Não há dúvidas hoje sobre a existência do efeito *filter-bubble* na esfera pública conectada. Com relação, no entanto, há escala e impacto desse efeito, encontramos opiniões distintas e as pesquisas nesse tema ainda são embrionárias. Além disso, a esfera pública conectada é altamente dinâmica, com seus algoritmos mudando constantemente, alterando o modo de funcionamento dos espaços de diálogo digital. Para Pablo Ortellado, baseando-se em estudo recente sobre o tema ("Avoiding the Echo Chamber about Echo Chambers, Knight Foundation", 2018): "O perigo dos guetos informacionais nas mídias sociais tem sido bastante superestimado. a polarização é um fenômeno circunscrito aos mais engajados, que são também os mais visíveis e os mais influentes nas mídias sociais. Ainda que alguns se sintam aliviados com essa constatação, ela não deveria trazer conforto. O sentimento de que a esfera pública é hoje um ambiente tóxico tomado por um diálogo de surdos não é uma ilusão criada pelas mídias sociais, que distorceriam uma realidade geral mais nuançada. Esses poucos que estão muito polarizados são aqueles que, por seu poder e influência, estruturam e organizam o debate público, tanto nas novas como nas velhas mídias. São eles também que, no final, orientam e informam os menos engajados, para o bem ou para o mal. As mídias sociais não parecem ser a causa da polarização política, nem nos EUA nem no Brasil. Mas o problema existe e não é uma miragem." Disponível em: <https://www1.folha.uol.com.br/colunas/pablo-ortellado/2018/02/polarizacao-na-internet-nao-parece-ser-causada-pelas-bolhas.shtml?utm_source=facebook&utm_medium=social&utm_campaign=compfb>. Acesso em: 29 abr. 2017.

[792] WU, Tim. *The Master Switch:* The Rise and Fall of Information Empires. Vintage. 2011.

Sabemos que a filtragem surgiu como uma necessidade e é muitas vezes considerada bem-vinda, gerando um comodismo muito grande ao usuário que encontra de forma rápida e eficaz, em grande parte das vezes, a informação ou qualquer outro conteúdo que deseja acessar. Este é o modelo de negócio do *Netflix*, por exemplo, que permite que usuário tenha à sua disposição um acervo de filmes baseado unicamente no seu perfil através da sugestão de títulos e filtros personalizados, com intuito de melhorar a experiência do usuário.

No entanto, para além da conveniência, o problema reside, no entanto, na forma e no excesso da filtragem, tanto por parte das empresas quanto dos próprios indivíduos que, sem ter consciência, se limitam e se afastam de pontos de vista divergentes dos seus, empobrecendo assim o valor do debate na esfera pública virtual. Por isso argumenta-se que os filtros-bolha limitam os usuários ao que desejam (ou desejariam) segundo, na maior parte das vezes, uma predição algorítmica. Isso dificulta o acesso às informações que deveriam ou precisariam ser vistas para o enriquecimento do debate democrático.

Além disso, em outra perspectiva, o usuário de Internet, ao navegar pelos sites mais conhecidos, é alvo hoje de uma torrente de publicidade direcionada que denota por si só o interesse comercial por trás deste mecanismo de filtragem e personalização.

A Internet é plástica e mutável e o fato de nos tornarmos involuntariamente reféns dos algoritmos que nos inserem dentro destas bolhas tem sido encarado com uma das mudanças mais drásticas, e sutis, por serem muitas vezes justamente imperceptíveis. A premissa do *filter bubble* é que você não decide deliberadamente o que aparece para você dentro da bolha, nem tem acesso ao que fica de fora.

É sabido que a curadoria de informação realizada pela mídia tradicional, nos meios off-line inclusive, já concretiza a ideia de filtragem de conteúdo selecionando, segregando uma série de informações. Habermas, assim como outros teóricos da Escola de Frankfurt, como Adorno e Horkheimer[793], já atentava para a força da mídia tradicional e seu impacto para a democracia moderna neste sentido[794].

[793] WIGGERSHAUS, Rolf, et al. *The Frankfurt School:* Its History, Theories, and Political Significance. The MIT Press, 1995.
[794] HABERMAS, Jürgen. op. cit., 2003, v. II, p. 99.

No entanto, muitas vezes as plataformas de Internet não possuem transparência suficiente no recorte informacional e algorítimico que realizam, dando uma falsa ideia ao consumidor de que as informações possuem um fluxo neutro e livre. Além disso, a filtragem por algoritmos que se vê nos ambientes on-line permite um grau de personalização e direcionamento em uma escala muito maior.[795] Com o advento da IoT, a problemática levantada a partir dos efeitos do filtro-bolha tende a se intensificar.

Na IoT, a interação com as plataformas digitais e com a inteligência artificial das Coisas atingirá um patamar ainda mais elevado, principalmente com a migração dos modelos de negócio de produtos para serviços. Tendo em vista a descrição prévia sobre o funcionamento dos negócios digitais baseados em dados e dos efeitos do filtro-bolha, a ideia de que a infraestrutura da Internet como esfera pública tem o potencial de permitir que as discussões possuam força suficiente para chegar a diferentes segmentos e a grupos de interesses diversos, replicando-se pelas várias redes de pessoas que compõem a sociedade, talvez seja uma realidade cada vez mais distanciada.

Isso se deve ao fato de que as expressões ficam muitas vezes restritas a uma mesma rede de pessoas com interesses comuns e com canais de comunicação facilmente manipuláveis pelos detentores das plataformas. A consequência disto é a intensificação da fragmentação comunicacional e a polarização do debate público.

Em uma visão habermasiana de legitimação do sistema político-democrático, este cenário é condenável tendo em vista que o fluxo comunicacional minimamente livre deve ser preservado no espaço público, permitindo que "todos os possíveis atingidos" tenham voz e participem de forma cada vez mais direta nas decisões, sejam elas pertinentes ao seu contexto privado ou politicamente na esfera pública.

No contexto tecnológico de Internet das Coisas, com cada vez mais dispositivos inteligentes conectados ao nosso redor, teremos ainda mais dados pessoais sendo recolhidos, armazenados e tratados. Em função disso, o processamento mercadológico de todas essas informações pode agravar ainda

[795] MAGRANI, Eduardo. *Democracia Conectada* - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.

mais o efeito *filter bubble* para atender a finalidades comerciais através de técnicas de *micro-targeting* e *profiling* de usuários.

Recentemente, um denunciante que trabalhava para obter dados de usuários no Facebook e repassar para a empresa Cambridge Analytica (contratada internacionalmente por diversos políticos em tempos eleitorais) concedeu depoimentos à imprensa revelando que 50 milhões de perfis foram colhidos para fins de manipulação política na esfera pública conectada.[796]

O denunciante, Christopher Wylie, descreveu como a empresa Cambridge Analytica ligada ao ex-assessor do presidente americano Donald Trump, gastou cerca de US$ 1 milhão na coleta de dados para enviar mensagens direcionadas a eleitores específicos, manipulando sua opinião política através de um algoritmo que conseguia analisar os perfis individuais e determinar traços de personalidade ligados ao comportamento online do eleitor, bem como seus sentimentos e medos, direcionado o conteúdo de manipulação sócio-política com base nesses fatores.[797]

Outrossim, com o ganho de maior sofisticação e autonomia das Coisas, nossa interação com esses agentes ficará cada vez mais simbiótica e complexa, trazendo à tona, ainda, uma maior capacidade de manipulação do nosso pensamento e comportamento.

Devemos somar a isso, como algo negativo, o fato de que não conhecemos muitas vezes como os algoritmos das Coisas inteligentes que compramos e dos espaços virtuais onde interagimos, funcionam[798]. O autor Frank Pasquale faz uma crítica a essa situação, tratando os algoritmos de hoje como

[796] Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 29 abr. 2017. Para entender melhor esse caso vide: http://irisbh.com.br/privacidade-no-facebook-cambridge-analytica/.

[797] Mesmo antes desse episódio, outros relatos importantes já foram dados sobre manipulação política através das esferas digitais. O artigo intitulado "Como Hackear uma Eleição", publicado pela Bloomberg Businessweek em 2016 relata como o hacker Andrés Sepúlveda fraudou eleições em toda a América Latina por quase uma década. Sepúlveda começou em 2005 desfigurando sites de campanha e invadindo bancos de dados de doadores dos oponentes políticos dos seus contratantes. Em poucos anos, ele estava montando equipes que espiavam, roubavam e difamavam em nome de campanhas presidenciais em toda a América Latina. Suas equipes trabalharam nas eleições presidenciais na Nicarágua, Panamá, Honduras, El Salvador, Colômbia, México, Costa Rica, Guatemala e Venezuela. Disponível em: < https://www.bloomberg.com/features/2016-how-to-hack-an-election/>. Acesso em: 29 abr. 2017. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 29 abr. 2017.

[798] PASQUALE, F. (2015). The Black Box Society: The secret algorithms that control money and information. Harvard University Press.

caixas pretas e jogando luz sobre os efeitos disso em uma sociedade guiada em diversas áreas por dados e decisões algorítmicas.[799]

Cada vez mais esses novos agentes não-humanos produzem efeitos em nossas ações ou mesmo tomam decisões importantes em nosso lugar através de customização da informação que nos é oferecida.

De forma geral, a tomada de decisões e a interação democrática comunicativa hoje estão passando por uma transformação profunda, pois estão sofrendo a intermediação e o agenciamento de agentes não-humanos, sejam eles Coisas, robôs ou algoritmos em si dotados de algum grau de inteligência artificial. Esses elementos estão influenciando nossa interação e nosso discurso com capacidade de produzir efeitos materiais de cunho político-democrático significativos, por isso devem ser melhor compreendidos para fins de regulação.

Nas discussões políticas, os robôs têm sido usados por todo o espectro partidário não apenas para conquistar seguidores, mas também para conduzir ataques a opositores e forjar discussões artificiais. Eles manipulam debates, criam e disseminam notícias falsas[800] e influenciam a opinião pública postando e replicando mensagens em larga escala. Muitos *bots*[801] (robôs)[802] têm replicado hashtags que ganham destaque com a massificação de postagens automatizadas de forma a sufocar debates espontâneos sobre um determinado tema.

[799] Recentemente, em Wisconsin no EUA, um juiz concedeu uma pena de prisão de seis anos levando em consideração na somente o registro criminal do réu, mas também sua pontuação na escala COMPAS (Correctional Offender Management Profiling for Alternative Sanctions). COMPAS é uma ferramenta algoritmica de que visa prever o risco de reincidência de um indivíduo. A pontuação sugeriu que o réu tinha um alto risco de cometer outro crime; assim, sua sentença de seis anos. O réu apelou da decisão, com o argumento de que o uso pelo juiz do algoritmo preditivo em sua decisão de sentença violou o devido processo e se pauta pela opacidade dos algoritmos. O caso foi para o Supremo Tribunal de Wisconsin. Disponível em: <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?mtrref=www.google.com.br&gwh=B3F9140AAAB1DACDFCE11CBD55F4DB8F&gwt=pay>. Acesso em: 29 abr. 2017.

[800] Sobre notícias falsas, recomenda-se a leitura da carta aberta defendida pelo grupo Coalizão de Direitos na Rede, trazendo guidelines sobre o assunto: Disponível em: <https://direitosnarede.org.br/p/carta-aberta-americalatinaecaribe-igf2017/>. Acesso em: 29 abr. 2017.

[801] O termo *Bot*, diminutivo de *Robot* (ou *Internet bot* ou *web robot*) é uma aplicação de software que tem o objetivo de oferecer um serviço automatizado para realizar tarefas em geral pré-determinadas. Eles imitam comportamentos humanos e vêm sendo utilizados na política e nas eleições para influenciar opinião em redes digitais, como em plataformas de redes sociais, mensagens instantâneas ou sites de notícias.

[802] Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/o-que-e-um-robo-na-web-e-como-ele-pode-influenciar-o-debate-nas-redes-especialistas-explicam.ghtml> Acesso em: 29 abr. 2017.

A princípio, as contas automatizadas podem até contribuir positivamente em alguns aspectos da vida nas redes sociais. Os *chatbots*[803] (chats operados por robôs), por exemplo, agilizam o atendimento a clientes de empresas e, em alguns casos, até auxiliam consumidores a processarem seus pedidos e obterem mais informações. Porém, um número crescente de robôs atua com fins maliciosos na esfera pública. Os robôs sociais (*social bots*) são contas controladas por softwares, que geram conteúdo artificialmente e estabelecem interações com não robôs. Eles buscam imitar o comportamento humano e se passar como tal de maneira a interferir em debates legítimos e voluntários e criar discussões forjadas.[804]

O crescimento da ação protagonizada por robôs representa, portanto, uma ameaça real para o debate público, representando riscos, no limite, à própria democracia, ao manipular o processo de formação de consensos na esfera pública e de seleção de representantes e agendas de governo.[805]

Corroborando com essa tese, em uma pesquisa recente, a Diretoria de Análise de Políticas Públicas (DAPP) da FGV [806] identificou interferências ilegítimas no debate online através do uso de *bots*. Contas programadas para

[803] Disiponível em: <https://medium.com/@tecnoequidade/especialistas-explicam-como-o-robô-pode-influenciar-o-debate-nas-redes-3a844f911849>. Acesso em: 29 abr. 2017.

[804] Disponível em: <http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web/>.

[805] Bots são responsáveis por mais de 50% do tráfego da Internet ao redor do mundo. Alguns bots têm como propósito, por exemplo, exigir prestação de contas de políticos, viralizar causas para a igualdade de gênero ou ajudar a organizar as (muitas) tarefas diárias de seus usuários. Já outros bots têm como objetivo espalhar mentiras para influenciar conversas na esfera pública, um fenômeno que desde 2014 vem ganhando escala global. Esses bots estão por aí e quase ninguém sabe como eles funcionam, quem os desenvolve e por quem são financiados. Para ilustrar essa questão, uma pesquisa recente demonstrou que a repercussão do cancelamento do evento do Queermuseu, exaustivamente comentada na imprensa nacional, foi insuflada por robôs na Internet. Dos mais de 700 mil tweets analisados, 8,69% foram disparados por bots, prejudicando a discussão pública. "Embora a decisão pelo cancelamento da exposição tenha levado em conta outros fatores, é possível dizer que a ação dos bots impactou na forma com que o debate foi conduzido, e suas consequências práticas. (...) O uso dos bots provoca um ambiente de polarização, uma vez que a internet tem um aumento no fluxo de mensagens com o mesmo teor. Neste cenário, assegura o pesquisador, fica difícil surgir um debate espontâneo, com ideias discordantes e moderadas. 'Esse tipo de ação dificulta o surgimento de posições mais moderadas. A busca de um consenso fica prejudicada porque os robôs conseguem sequestrar parte do debate'". Disponível em: <https://g1.globo.com/rs/rio-grande-do-sul/noticia/pesquisa-demonstra-que-repercussao-do-cancelamento-do-queermuseu-foi-insuflada-por-robos-na-internet.ghtml>. Acesso em: 2 mar. 2017.

[806] Disponível em: <http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf>. Acesso em: 29 abr. 2017.

postagens massivas se converteram em uma potencial ferramenta para a manipulação de debates nas redes sociais.[807]

> No Brasil, a Pesquisa Brasileira de Mídia 2016, realizada pela Secretaria Especial de Comunicação Social (Secom) da Presidência da República, revela que 49% das pessoas já se informam pela internet, uma fatia em rápido crescimento. É nesse ambiente de "confiança", mas de alta circulação de informações duvidosas que os robôs se proliferam.[808]
> (...)
> O estudo feito pela FGV/DAPP aponta que esse tipo de conta (perfis de bots) chegou a ser responsável por mais de 10% das interações no Twitter[809] nas eleições presidenciais de 2014. Durante protestos pelo Impeachment, essas interações provocadas por robôs representaram mais de 20% do debate entre apoiadores de Dilma Rousseff, que usavam significativamente esse tipo de mecanismo. Um outro exemplo analisado mostra que quase 20% das interações no debate entre os usuários favoráveis a Aécio Neves no segundo turno das eleições de 2014 foi motivado por robôs.[810]

Com este tipo de manipulação, os robôs criam a falsa sensação de amplo apoio político a certa proposta, ideia ou figura pública, modificam o rumo de políticas públicas, interferem no mercado de ações, disseminam rumores, notícias falsas e teorias conspiratórias, geram desinformação e poluição de conteúdo, além

---

[807] Disponível em: <http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web/>. Acesso em: 29 abr. 2017.

[808] Disponível em: <http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf>. Acesso em: 29 abr. 2017.

[809] Bot são programas de computador criados para executar tarefas específicas. Os primeiros robôs não tinham intenções maliciosas, mas no final da década de 1990 os bots começaram a desenvolver uma reputação mais negativa. Alguns bots têm sido usados em ataques de negação de serviço (DDoS), e-mails de spam, roubo de identidade em massa e ataques de desinformacao para manipulacao na esfera publica. Um Twitter Bot é uma conta controlada por um algoritmo ou script, normalmente utilizadas para realizar tarefas repetitivas, por exemplo, retweetar conteúdo contendo palavras-chave particulares, responder a novos seguidores e enviar mensagens diretas a novos seguidores. Twitter Bots mais complexos podem participar de conversas online e, em alguns casos, tem um comportamento muito parecidos ao comportamento humano. As contas bot compõem entre 9 e 15% de todas as contas ativas no Twitter, mas estudos mais aprofundados indicam que este percentual pode ser ainda maior devido a dificuldade de identificar os bots complexos. Os bots do Twitter geralmente não são criados com intenção maliciosa; eles são freqüentemente usados para bate-papo on-line ou para aumentar o impacto do perfil corporativo, mas sua capacidade de permear nossa experiência on-line e moldar o discurso político garante a eles um novo poder de agência e por isso merecem maior atenção e escrutínio.

[810] "Apesar de os robôs operarem a favor de agendas específicas, isso não quer dizer que dominem completamente a rede nem que a percepção final da maior parte das pessoas será resultante direta da influência desses dispositivos. O que constatamos, no entanto, é que eles existem, já operam no debate brasileiro, obedecem padrões e buscam influenciar. Sobretudo, esse esforço de pesquisa aqui apresentado busca emitir um alerta de que não estamos imunes e que devemos nos preocupar em buscar entender, filtrar e denunciar o uso e a disseminação de informações falsas ou manipulativas por meio desse tipo de estratégia e tecnologia. Deve-se ter atenção e proteger os espaços democráticos inclusive nas redes sociais." Disponível em: <http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf>. Acesso em: 29 abr. 2017.

de atrair usuários para links maliciosos que roubam dados pessoais, entre outros riscos.[811]

Ao interferir em debates em desenvolvimento nas redes sociais, robôs estão atingindo diretamente os processos políticos e democráticos através da influência da opinião pública. Suas ações podem, por exemplo, produzir uma opinião artificial, ou dimensão irreal de determinada opinião ou figura pública, ao compartilhar versões de determinado tema, que se espalham na rede como se houvesse, dentre a parcela da sociedade ali representada, uma opinião muito forte sobre determinado assunto.[812] [813]

Segundo o estudo:[814]

> Isso acontece com o compartilhamento coordenado de certa opinião, dando a ela um volume irreal e, consequentemente, influenciando os usuários indecisos sobre o tema e fortalecendo os usuários mais radicais no debate orgânico, dada a localização mais frequentes dos robôs nos polos do debate político. Os perfis automatizados também promovem a desinformação com a propagação de notícias falsas e campanhas de poluição da rede. Robôs frequentemente usam as redes sociais para reproduzir notícias falsas com o objetivo de influenciar determinada opinião sobre uma pessoa ou tema, ou poluir o debate com informações reais, porém irrelevantes para a discussão em questão. Esta ação, que conta com o compartilhamento de links como principal mecanismo de propagação, tenta evitar

[811] Sobre a existência hoje de um "exército" de perfis falsos, vide: http://www.bbc.com/portuguese/brasil-42172146. Acesso em: 14 mar. 2018.

[812] Disponível em: <http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf>. Acesso em: 29 abr. 2017.

[813] Segundo Danilo Doneda e Yasodara Córdova: (...) se os bots existem em grande número, implicando elevado volume de informações, é possível que possam direcionar o fluxo dessas informações em redes sociais, pois algoritmos presentes em nessas plataformas geralmente priorizam o elemento quantitativo, não distinguindo entre bots e humanos. Desse modo também, muitas pessoas podem formar suas ideias e convicções – e decisões quanto ao próprio voto – a partir de direções que seus grupos sociais estão tomando, eventualmente influenciados por informação direcionada por bots. (...) A utilização de bots em redes sociais durante as eleições é realidade no Brasil ao menos desde o pleito de 2010 e o seu uso tem sido cada vez mais debatido em relação à possibilidade de que afetem, positiva ou negativamente, o debate democrático. Esse debate se dá em meio à recente divulgação de diversas situações nas quais bots e outros mecanismos teriam sido responsáveis por moldar o perfil do fluxo de informação no debate público em redes sociais, eventualmente influenciando concretamente no resultado de pleitos eleitorais como o norte-americano, o separatismo catalão ou a saída do Reino Unido da União Europeia. Ao mesmo tempo, ainda não há métodos infalíveis que permitam medir concretamente a extensão desta influência e as modalidades pelas quais ela opera, o que sugere que esta questão seja abordada com atenção porém também com muita prudência, afim de que qualquer forma de regulação não inviabilize utilizações legítimas dos bots". CÓRDOVA, Yasodara e DONEDA, Danilo. Um lugar para os robôs (nas eleições). JOTA. 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017>. Acesso em: 09 mar. 2018. Há hoje Projetos de Lei tramitando no Brasil em âmbito federal para proibir a utilização e contratação de bots para fins eleitorais. Vide: https://www.tecmundo.com.br/seguranca/123637-senador-quer-criminalizar-uso-robos-internet-campanha-politica.htm. Acesso em: 29 abr. 2017.

[814] Ibid.

ou diminuir o peso do debate sobre determinado assunto. Para isso, os robôs geram um número enorme de informações, que chegam até os usuários simultaneamente às informações reais e relevantes, que acabam tendo seu impacto diminuído.

Segundo a Pesquisa da FGV: [815]

Os robôs têm maior facilidade de propagação no Twitter do que no Facebook por uma série de motivos. O padrão de texto do Twitter (140 caracteres) gera uma limitação de comunicação que facilita a imitação da ação humana. Além disso, o uso de @ para marcar usuários, mesmo que estes não estejam conectados a sua conta na rede, permite que os robôs marquem pessoas reais aleatoriamente para inserir um fator que se assemelhe a interações humanas. Robôs também se aproveitam do fato de que, geralmente, as pessoas são pouco criteriosas ao seguir um perfil no Twitter, e costumam agir de maneira recíproca quando recebem um novo seguidor. Experimentos mostram que no Facebook, plataforma na qual as pessoas costumam ser um pouco mais cuidadosas ao aceitar novos amigos, 20% dos usuários reais aceitam pedidos de amizade de maneira indiscriminada, e 60% aceitam sempre que possuem ao menos um amigo em comum. Dessa maneira, os robôs adicionam um grande número de pessoas ao mesmo tempo e seguem páginas reais de pessoas famosas, além de seguir e serem seguidos por um grande número de robôs, de forma que acabam criando comunidades mistas - que incluem perfis reais e falsos (Ferrara et al., 2016).

Alguns robôs pretendem apenas desviar a atenção para um determinado tema e, por isso, se preocupam menos com a sua similaridade com um usuário humano do que com a intensidade e a capacidade de modificar o rumo do debate nas redes. Outros mecanismos, contudo, possuem uma série de estratégias para imitar o comportamento humano e, assim, serem reconhecidos como tal, tanto por usuários, quanto por sistemas de detecção.

Sabendo que o comportamento humano nas redes sociais tem algum padrão temporal na produção e no consumo de conteúdo, os perfis são programados para postar de acordo com essas mesmas regras. Paradoxalmente, é justamente a falta de padrão tanto temporal quanto de conteúdo no longo prazo que os robôs têm mais dificuldade de imitar, e o que costuma permitir a sua identificação (Brito, Salvador e Nogueira, 2013).

Os algoritmos mais modernos vão além: conseguem identificar perfis populares e segui-los, identificar um assunto sendo tratado na rede e gerar um pequeno texto por meio de programas de processamento de linguagem natural (natural language algorithms) e gerar certo grau de interação. Nesse sentido, pesquisas concluem que as atividades das contas robôs tendem a ser menos complexas na variedade de ações que praticam, o que adiciona mais uma possibilidade à combinação de fatores que permite que se afirme categoricamente que um determinado perfil é um robô. Esse tipo de sistema, por combinar diferentes dados, também obtém bons resultados a partir de um número menor de informações – como os 100 últimos tweets –, o que acelera a análise e a capacidade de processamento.[816]

[815] Disponível em: <http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf>. Acesso em: 29 abr. 2017.
[816] Disponível em: <http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf>. Acesso em: 29 abr. 2017.

O estudo do uso de robôs no período analisado[817] já demonstra de forma clara o potencial danoso dessa prática para a disputa política e o debate público. Uma das conclusões mais evidentes nesse sentido é a concentração dessas ações em polos políticos localizados no extremo do espectro político, promovendo artificialmente uma radicalização do debate nos filtros-bolha e, consequentemente, minando possíveis pontes de diálogo entre os diferentes campos políticos constituídos. Assim, a atuação de robôs não apenas dissemina notícias falsas, que podem ter efeitos nocivos para a sociedade, mas também busca ativamente impedir que os usuários se informem de maneira adequada.

Outra estratégia comum dos perfis automatizados é o compartilhamento de links maliciosos, que tem como fim o roubo de dados ou informações pessoais. Essas informações – como fotos de perfil - podem ser usadas para a criação de novos perfis robôs que tenham características que os auxiliem a iniciar conexões nas redes com usuários reais. Uma ação comum, que costuma gerar suspeita sobre a atuação de robôs, é a marcação por parte de um usuário desconhecido.

Este tipo de atuação sugere que as redes sociais, usadas por tantas pessoas para fins de informação, podem estar na verdade contribuindo para uma sociedade menos informada, manipulando o debate público. Somados, esses riscos e outros representados pela ação de artefatos *não-humanos* (como *bots*), são mais do que o suficiente para jogar luz sobre uma ameaça real à qualidade do debate na esfera pública.[818]

[817] Segundo a pesquisa: "A detecção através de aprendizado de máquinas ocorre com a codificação de padrões de comportamento a partir da coleta de metadados. Desta forma, o sistema é capaz de identificar automaticamente humanos e robôs com base no padrão comportamental do perfil. Os metadados dos usuários são considerados um dos aspectos mais previsíveis para diferenciar humanos e robôs e podem contribuir para uma melhor compreensão do funcionamento de robôs mais sofisticados. Identificar esses robôs ou contas hackeadas, no entanto, é difícil para estes sistemas. Além disso, a evolução constante dos robôs faz com que o sistema, construído a partir de uma base de dados estática, se torne menos preciso ao longo do tempo. No entanto, ele permite processar um grande número de correlações e padrões complexos, além de analisar um grande número de contas. Os mecanismos mais eficientes de identificação combinam diferentes aspectos dessas abordagens, explorando múltiplas dimensões do comportamento do perfil, como atividade e padrão de horário. Estes sistemas levam em conta, por exemplo, que usuários reais passam mais tempo na rede trocando mensagens e visitando o conteúdo de outros usuários, como fotos e vídeos, enquanto contas robôs passam o tempo pesquisando perfis e enviando solicitações de amizade." Disponível em: <http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf>. Acesso em: 29 abr. 2017.

[818] Para Habermas, devemos atingir ao máximo as condições de fala ideal, isto é, conseguir criar um ambiente de deliberação democrática em que todos tenham voz. Diante de um cenário de crise de representatividade, a Internet deve ser utilizada como ferramenta para que o cidadão exerça a

Além disso, os artefatos não-humanos vêm ganhando cada vez mais autonomia e imprevisibilidade comportamental. Um bom exemplo para explicar os efeitos danosos que um elemento não-humano pode ter é o caso do robô Tay.

Em 2016, a *Microsoft* lançou um *chatbot* - um programa de Inteligência Artificial -, denominado Tay. Dotado de capacidade *deep learning*, o robô moldava sua visão de mundo baseando-se na interação online com outras pessoas e produzindo expressões autênticas a partir delas. A experiência, contudo, se mostrou desastrosa, e a companhia teve de desativar a ferramenta menos de 24 horas depois do início de seu funcionamento em razão da produção resultados preocupantes.

Palavras que configuram discursos de ódio contra minorias historicamente marginalizadas foram proferidas. Tay afirmou, por exemplo, que Hitler estava certo e que ela odiava judeus. Adicionalmente, disse que odeia feministas e que elas deveriam "morrer e queimar no inferno".

Esse consiste em um bom exemplo que conjuga as importantes discussões travadas neste trabalho, como: o tratamento de informações dos usuários para alimentar o funcionamento de uma Coisa inteligente, com capacidade de interagir e influenciar de maneira imprevisível na esfera pública conectada.

Esses exemplos nos alertam para o fato de que o papel democrático da esfera pública conectada começa a esbarrar em riscos e obstáculos que podem reduzir consideravelmente seu potencial, além de não dever ser encarada entusiasticamente como a panaceia para a salvação da legitimidade do sistema político contemporâneo.

A influência hipertrófica da racionalidade econômica do mercado e burocrática do sistema político nas esferas do mundo da vida é encarada por Habermas como uma das principais patologias da modernidade, levando a perdas de liberdade e de sentido na sociedade.

---

sua cidadania de maneira ativa. Segundo Habermas, para a deliberação democrática ocorrer, há pelo menos quatro condições. Estas condições, caracterizadoras de uma "situação ideal de fala", estão atreladas basicamente à necessidade de se garantirem as melhores condições de deliberação e à preocupação com a forma como se organiza o processo de debate. São elas: (i) cada pessoa precisa estar hábil a expressar suas próprias ideias abertamente e criticar as dos outros; (ii) a associação dos conceitos de força e poder com status social precisa ser eliminada; (iii) argumentos baseados no apelo à tradição ou dogma precisam ser expostos; e (iv) a verdade é alcançada por meio da busca ao consenso. "

Por isso, o inicial frenesi com o ideal de esferas virtuais democráticas e descolonização do mundo da vida propiciada pelos novos ambientes digitais tem perdido fôlego. Agora que os algoritmos e demais agentes não-humanos estão participando e influenciando os discursos na esfera pública, cabe a indagação: serão eles obrigados a agirem moralmente e de forma racional-dialógica na comunicação para não afetar negativamente a situação ideal de fala?[819]

Muitas vezes não há uma consciência crítica sobre como os algoritmos que compõem as Coisas funcionam, sempre visando compreender como podem nos oferecer informações personalizadas a partir dos nossos dados pessoais ou mesmo manipular nossa visão política. É importante termos em mente que esse funcionamento muitas vezes atende a disputas políticas ou a modelos de negócio privados que visam maximizar lucro e não necessariamente concretizar direitos fundamentais como acesso à informação, expressão e cultura.

A teoria habermasiana fundamentada nos conceitos comunicacionais racionais e dialógicos de esfera pública e situação ideal de fala, nos ajuda a observar o quanto estamos nos distanciando, no contexto de IoT, de um cenário positivo do ponto de vista da legitimidade democrática. Pela analise feita, podemos compreender a atual situação como uma colonização do mundo da vida reforçada por meio de agentes não-humanos (Coisas, *Bots*, algoritmos com inteligência artificial, entre outros), produzindo efeitos nocivos agravados pelos

[819] Nas palavras de Marcelo Fraga: Jürgen Habermas, na construção de sua teoria crítica da sociedade, entende necessário aprofundar o exame da própria racionalidade e desenvolve a sua *Teoria da Ação Comunicativa* como elemento de compreensão para a fundamentação da *Ética do Discurso*. A *Ética do Discurso* é uma teoria da moral que recorre à *razão* para sua fundamentação. Habermas parte do conceito de *razão reflexiva* de Kant para desenvolver o conceito de *razão comunicativa*. Enquanto na razão kantiana o juízo categórico está fundado no sujeito e supõe uma razão monológica, a *razão comunicativa* está centrada no diálogo, na interação entre os indivíduos do grupo, mediada pela linguagem e pelo discurso. A *razão comunicativa*, em complemento à *razão reflexiva* (aquela apenas do indivíduo) é enriquecida exatamente por ser processual, construída pela interação entre os sujeitos enquanto seres que se posicionam criticamente frente às normas. A validade das normas, portanto, não deriva de uma razão abstrata e universal, tampouco depende da subjetividade de cada um, mas do consenso encontrado a partir do grupo, da interação do conjunto dos indivíduos participantes de um debate e, nesse processo, a subjetividade se transforma em intersubjetividade. Contudo, do ponto de vista da *razão comunicativa*, a interação entre os sujeitos precisa ser estabelecida sem as pressões típicas dos sistemas econômico e político da sociedade moderna, que se fundam, de certa maneira, na força do dinheiro e no exercício do poder. A *ação comunicativa* supõe o entendimento entre os indivíduos que buscam, pelo uso de argumentos racionais, convencer o outro a respeito da validade da norma, permitindo um avanço para uma sociedade baseada na espontaneidade, na solidariedade e na cooperação. Disponível em: <https://esbocosfilosoficos.com/2013/02/23/o-que-e-iluminismo/>. Acesso em: 29 set. 2017.

efeitos de filtro-bolha e de radicalização dos discursos. A regulação jurídica precisa estar atenta a esses efeitos, buscando corrigi-los.

Para aprofundarmos as possíveis soluções para esses problemas, no entanto, a teoria habermasiana isoladamente não nos auxilia de forma suficiente. Isso se deve ao fato de que esta foi pensada principalmente para medir e induzir o comportamento do agente humano racional e dialógico que interage na esfera pública.

Portanto, ao possuir essa lente iluminista, Habermas não nos permite identificar diversos elementos não-humanos dotados de real poder de agência, capazes de interagir e de influenciar outros atores de forma cada vez mais autônoma, dignos de serem observados quando tratamos de esfera pública.

Para aprofundarmos o estudo destes elementos, buscando compreender melhor seu impacto no próprio sistema democrático, devemos então sobrepor essa lente de matriz iluminista para que tais agentes apareçam no campo de visão da esfera pública. Para isso, exploraremos, no item seguinte, novas lentes teóricas para uma análise mais adequada à era da hiperconectividade.

3.3
Possíveis Soluções para uma Miopia Ontológica e Epistemológica na Era da Hiperconectividade

Na era da hiperconectividade, nosso comportamento e visão de mundo passam a ser moldados através da interação com agentes não-humanos, cada vez mais autônomos, inteligentes e imprevisíveis. Além disso, dotados de tecnologias progressivamente mais complexas e difíceis de se compreender em termos de funcionamento, riscos e potencialidades. Essa constante interação, por sua vez, sustenta-se no intenso fluxo de informações, descrito de forma aprofundada no capítulo anterior, levantando preocupações legítimas relacionadas não somente à proteção da privacidade e segurança dos usuários, mas também a questões éticas que precisam de um enquadramento mais adequado para serem endereçadas.

A teoria habermasiana nos fornece um importante parâmetro para pensarmos sobre a legitimidade das leis e do sistema político-democrático em que vivemos, pensado a partir de um processo de deliberação e convencimento mútuo e racional na esfera pública. Porém, essa teoria não nos permite identificar

diversos elementos não-humanos como atores sociais capazes de agir, interagir e nos influenciar, isto é, como um fenômeno digno de ser observado quando tratamos de esfera pública. Há, portanto, na teoria habermasiana, uma miopia ontológica[820] e epistemológica[821] para se entender os efeitos deste novo contexto tecnológico.

A insuficiência relativa da lente deontológica habermasiana para se pensar a dinâmica da esfera pública na era da hiperconectividade, nos leva à necessidade neste trabalho de pensarmos em novas sobreposições teóricas que nos permitam compreender e regular adequadamente o universo de IoT.

No contexto de IoT, a ação dos algoritmos e componentes físicos, como sensores e demais "Coisas" inteligentes, pode ser vista em uma perspectiva de capacidade de agência e decisão mais ampla e complexa. Os algoritmos hoje não só prevêem os próximos livros de best-sellers, mas também sugerem nossos futuros parceiros amorosos, influenciam nossas decisões eleitorais, criam ameaças de morte, decidem quem deve ser preso e compram drogas ilegais na *Deep Web*.[822]

Sobre as influências possíveis a partir da interação com essas novas Coisas, uma interessante e recente pesquisa[823] despertou a atenção da imprensa ao afirmar que crianças estão ficando mal-educadas como consequência da interação com *bots*. A razão seria que a comunicação com esses dispositivos é sempre feita na forma de comandos imperativos: "Apague as luzes", "toque uma música" e assim por diante. Palavras fundamentais para a comunicação humana respeitosa, como "por favor" e "obrigado", ficam de fora da comunicação.

Portanto, segundo a pesquisa, na medida em que as crianças estão interagindo cada vez mais com assistentes de voz (dispositivos criados para

[820] A miopia *ontológica* neste contexto se deve ao enclausuramento da teoria habermasiana em sua matriz antropocêntrica e iluminista, o que conduz a uma dificuldade intrínseca de compreender com clareza teórica suficiente a realidade e existência dos entes não-humanos e sua influência na sociedade hiperconectada.

[821] A miopia *epistemológica* neste contexto se deve à limitação de se aplicar a teoria democrática habermasiana isoladamente, para se tecer uma teoria do conhecimento aplicada a agentes não-humanos, devido à sua concepção fortemente iluminista e antropocêntrica.

[822] Disponível em: <http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf>. Acesso em: 29 set. 2017.

[823] Disponível em: <https://www.washingtonpost.com/local/how-millions-of-kids-are-being-shaped-by-know-it-all-voice-assistants/2017/03/01/c0a644c4-ef1c-11e6-b4ff-ac2cf509efe5_story.html?utm_term=.4cb453261fa8>. Acesso em: 29 set. 2017.

executar instruções e até mesmo conversar com o usuário em linguagem natural),[824] acabam trazendo o mesmo hábito para as interações humanas. Por exemplo, gritando ou dando ordens imperativas para os pais, amigos e professores, como se eles também fossem assistentes virtuais robotizados.[825]

Segundo a pesquisa, muitos pais estão notando essa deseducação dos próprios filhos, que reproduzem a forma de comunicação entre os pais e as máquinas. Esse é um exemplo de como as Coisas podem exercer uma influência real em nosso comportamento e por isso exigem melhor compreensão para pensarmos em diretrizes éticas para o seu desenvolvimento.[826]

Além disso, não basta apenas perceber a capacidade dos algoritmos de agir e decidir como seres humanos. É necessário pensar sobre como a esfera pública está sendo influenciada por esses agentes capazes de moldar, estruturar e mediar a maneira como interagimos. Para uma compreensão adequada deste fenômeno, a análise de uma esfera pública baseada unicamente na racionalidade comunicativa humana é insuficiente, conforme sustentado anteriormente.

Essa perspectiva advém principalmente da tradição filosófica humanista clássica - perspectiva que entende o homem como o centro de todas as relações estabelecidas em comunidade. Diante de lentes teóricas como a habermasiana, nos deparamos com uma miopia ontológica e epistemológica que nos impede de compreender e gerenciar adequadamente os efeitos da hiperconectividade, contexto esse em que a agência de atores não-humanos representa efeitos materiais concretos e significativos.

Em crítica à visão de mundo humanista, Michel Foucault, um dos grandes nomes do pós-estruturalismo, analisou o que chamou de "a morte do homem". Na última parte de sua obra, "A ordem das coisas", Foucault anuncia que logo o homem desaparecerá. Nas palavras do autor:[827]

---

[824] Disponível em: <https://www.washingtonpost.com/local/how-millions-of-kids-are-being-shaped-by-know-it-all-voice-assistants/2017/03/01/c0a644c4-ef1c-11e6-b4ff-ac2cf509efe5_story.html?utm_term=.4cb453261fa8>. Acesso em: 29 set. 2017.

[825] Disponível em: <http://www1.folha.uol.com.br/colunas/ronaldolemos/2017/11/1936624-como-falar-com-as-maquinas.shtml>. Acesso em: 18 out. 2017.

[826] Uma solução de ética by design nesse caso, por exemplo, seria programar o artefato técnico para exigir palavras educadas como por favor e obrigado das crianças durante a interação. Além do conceito de ética by design, essa discussão traz à tona também a necessidade de pensarmos em "algoritmos empáticos" para as Coisas inteligentes, buscando interações cada vez mais saudáveis entre homens e máquinas.

[827] Les Mots et les choses (The Order of Things, 1966).

> O homem é uma invenção recente. E talvez perto de seu fim. Se esses arranjos desaparecessem à medida que aparecem, se algum evento do qual, até o momento, não temos conhecimento algum, senão mera percepção de sua possibilidade – não sabendo qual será sua forma, ou o que promete – causasse seu desmoronamento, assim como da base do pensamento clássico, no final do século XVIII, pode-se certamente apostar que o homem seria apagado, como um rosto desenhado na areia à beira do mar.[828]

O pensador francês anuncia a morte do homem no mundo pós-moderno, assim como Nietzsche havia proclamado a morte de Deus em sua obra "A Gaia Ciência", um século antes, ao analisar o enfraquecimento dos valores cristãos no mundo ocidental. Nietzsche reconheceu a crise que a morte simbólica de Deus representava para os pressupostos morais existentes. A morte de Deus seria uma maneira de dizer que os humanos e a civilização ocidental como um todo não poderiam mais acreditar em tal ordem, podendo isso levar a sociedade não só à rejeição de uma crença de ordem cósmica ou física, mas também a uma rejeição dos próprios valores absolutos.

Tratando de um contexto diferente, Michel Foucault chama atenção para a importância de percebermos o impacto dos agentes não-humanos (como Coisas, algoritmos, entre outros) nas esferas de poder, em superação à ótica iluminista antropocêntrica.

O estudo de Foucault sobre as relações de poder em sociedade se deu em grande parte sobre a ideia do conhecimento e como ele é aplicado. O debate sobre o conhecimento como fonte de um exercício de poder necessariamente passa pela consideração da ciência e de suas descobertas como mecanismos diretamente ligados à dinâmica de poder estabelecida, de modo que seria impossível "dissociar as experiências técnicas ou científicas dos regimes de poder dentro dos quais operam".[829]

O pensamento entendido como pós-humanista vem buscando compreender e tecer novas concepções sobre o distanciamento da ideia que temos de condição

---

[828] Tradução livre do autor. No original: *Man is an invention of recent date. And one perhaps nearing its end. If those arrangements were to disappear as they appeared, if some event of which we can at the moment do no more than sense the possibility – without knowing either what its form will be or what it promises – were to cause them to crumble, as the ground of Classical thought did, at the end of the eighteenth century, then one can certainly wager that man would be erased, like a face drawn in sand at the edge of the sea.*

[829] WEINBERG, Darin. Social Constructionism. In: Bryan S. Turner (Ed.). *The new blackwell companion to social theory*. Chichester, UK: Wiley-Blackwell, 2009. p. 281-299.

humana e das tradicionais limitações ínsitas a nós, como morte e doenças, que poderiam ser em breve superadas. Segundo essa perspectiva, essa nova condição, impulsionada pelos avanços da tecnologia, coloca em xeque uma série de perspectivas filosóficas de matriz humanista e iluminista e nos força a repensar nossa ontologia.

Estudiosos indicam que o advento do pensamento pós-humanista teria se dado na década de 1970, quando a teoria dita anti-humanista estava se difundindo e o humanismo enfrentava o início das contribuições pós-humanistas. Na expansão desta perspectiva, o progresso técnico e a criação artística tiveram intensa conexão. Segundo Francisco Rüdiger[830], William Gibson cunhou o termo em seus contos de ficção-científica do início dos anos 1980 e, assim, transmitiu-nos a ideia de ciberespaço. Arthur Clarke, por sua vez, escreveu sobre a descarga da mente em computadores no livro *The city and the stars* (1956).

Em *Marooned in Realtime* (1986), Vernor Vinge elaborou a expressão "singularidade tecnológica", que hoje motiva os interessados no desenvolvimento de uma inteligência supra-humana. Em 1952, Van Vogt sugeriu o termo pós-humano, para designar uma outra raça criada pelo ser humano em seu conto *Slan*. Em bases ensaísticas, o sentido que o termo passou a ter em seguida parece, porém, ter sido explorado pela primeira vez por James Bernal, em 1929 (*The World, the Flesh and the Devil: An Enquiry into the Future of the Three Enemies of the Rational Soul*). Paralelamente, o conceito de ciborgue passou a ser utilizado, encontrando referências em autores como Donna Haraway.[831]

Com isso, a partir da década de 1980, a teoria pós-humanista começou a se delinear de forma mais estruturada, tendo contado com a contribuição de Hans Morave, Eric Drexler e Marvin Minsky[832], e a ideia de transferir a mente humana para uma rede neuronal artificial ganhou corpo. Contudo, destaca Francisco Rüdiger, o pós-humano, muito mais do que dispor de próteses acopladas ao corpo,

---

[830] RÜDIGER, Francisco. Breve história do pós-humanismo: elementos de genealogia e criticismo. *Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação*, v. 8, p. 6, abr. 2007.

[831] Cf. HARAWAY, Donna. A cyborg manifesto: Science, technology and socialist-feminism in the late twentieth century. In: _____. *Simians, Cyborgs, and Women*. The Reinvention of Nature. Nova York: Routledge, 1991.

[832] Cf. REGIS, Edward. *Great Mambo Chicken and the Transhuman Condition*: science slightly over the edge. Woburn(MA): Perseus Books, 1990 *apud* RÜDIGER, Francisco. Breve história do pós-humanismo: elementos de genealogia e criticismo. *Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação*, v. 8, p. 09, abr. 2007.

relaciona-se com a nossa subjugação ao pensamento tecnológico da atualidade, o pensamento cibernético.[833]

Tanto a visão crítica pós-estruturalista quanto pós-humanista e suas derivações merecem atenção renovada na Era Digital pautada pelo avanço da Internet das Coisas e da Inteligência Artificial. Hoje, agentes não-humanos (como os algoritmos com capacidade de *deep learning* e auto-programação) possuem capacidade de agência significativa podendo influenciar e serem influenciados na esfera pública conectada, gerando desinformação, manipulação e extremismo nos espaços digitais. Esse fenômeno é novo na história da humanidade e representa um ponto cego em várias teorias críticas, como a teoria habermasiana, que deve, portanto, ser complementada por novas lentes epistemológicas e ontológicas necessárias para repensar pressupostos sobre agência, transparência e normatividade desses atores, bem como sobre o papel desses sistemas nos processos democráticos.

Essa abordagem é imprescindível para se assegurar diretrizes éticas adequadas aos avanços da tecnologia e da hiperconectividade. Pretende-se, por meio desta perspectiva, conseguir abordar as seguintes reflexões: (i) O que há de novo no fenômeno de interação entre humano e não-humano?; (ii) As tecnologias e as Coisas devem ter status diferente considerando sua capacidade de interação / agência / impacto na esfera pública?; (iii) Como deve ser a responsabilidade desses agentes não-humanos considerando seu status na rede sociotécnica? Exploraremos todas essas questões a seguir.

3.3.1
A Teoria ator-rede e O Novo materialismo das coisas

As interações dos algoritmos com a sociedade têm provocado influências crescentes na cultura, na política e nas relações sociais. No atual contexto de grande desenvolvimento tecnológico e do estabelecimento de um quadro de crescente conectividade e do uso cada vez mais frequente de novas Coisas

[833] RÜDIGER, Francisco. Breve história do pós-humanismo: elementos de genealogia e criticismo. *Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação*, v. 8, p. 10, abr. 2007.

conectadas na vida das pessoas, é notável que os algoritmos passam a exercer um impacto nas sociedades contemporâneas.

Os algoritmos não apenas realizam projeções, como têm também sido crescentemente aplicados em processos de tomada de decisão. Dessa forma, também tem demonstrado ter uma capacidade de agência significativa, podendo ter a capacidade de influenciar e afetar outros agentes na esfera pública. Para nos ajudar a identificar esses novos atores da esfera pública, a teoria do antropólogo francês Bruno Latour representa um salto importante.

Latour joga luz justamente sobre o obstáculo teórico abordado acima, nos ajudando a compreender a influência que os dispositivos tecnológicos possuem em nossa sociedade, superando a ideia de que o poder de agência é exercido apenas por pessoas.

Distanciando-se da teoria habermasiana, o teórico Bruno Latour entende que objetos são dotados de agência e propõe a superação da categorização binária humano/não-humano. A visão de Latour ampara-se em um entendimento teórico que rejeita a modernidade e suas características[834]. Vale dizer, adota-se uma postura contra o pensamento do período iluminista. Como se sabe, na modernidade, buscava-se a "auto-emancipação de uma humanidade razoável"[835] e características como racionalismo, universalismo e exaltação do intelecto humano davam os contornos principais ao século das luzes.

Latour rejeita esses pilares, pois, por mais que neste período tenha havido grande crescimento da ciência (com suas conotações de racionalidade e progresso) e a quebra de tabus, a esperança pautada na ideia de que seres humanos são guiados pela razão[836] não foi capaz de impedir as horríveis guerras e os campos de concentração[837]. Para Latour, o conceito de modernidade ou de racionalidade

[834] LATOUR, Bruno. *Jamais Fomos Modernos*: Ensaio de Antropologia Simétrica. Trad.: Carlos Ireneu da Costa. Rio de Janeiro: Editora 34, 1994.
[835] ROUANET, Sergio Paulo. *Mal-estar na modernidade*. São Paulo: Companhia das Letras, 1993, p. 97.
[836] Sobre a racionalidade na modernidade, Boaventura de Souza Santos afirma que ela se dividia em três – racionalidades estético-expressiva, moral-prática e cognitivo-instrumental – para sustentar o pilar da emancipação presente no pensamento da época. SANTOS, Boaventura de Souza. *Pela mão de Alice*: O social e o político na pós-modernidade. 7. ed. Porto: Edições Afrontamento, 1999, p. 76 e ss.
[837] FEENBERG, Andrew. Modernidade, Tecnologia e Formas de Racionalidade. In: _____. *Tecnologia, Modernidade e Democracia*. Org. e trad.: Eduardo Beira. Lisboa: MIT Portugal/ IN+/ Inovatec, 2015, pp. 191 e 193.

humana não teria qualquer conteúdo preciso[838]. Em suma, Latour rompe com os ideais iluministas e passa a integrar uma ótica diferente do materialismo clássico, buscando analisar o significado de ser um indivíduo material que possui necessidades biológicas e vive num mundo em que há objetos naturais e artificiais, além de micro-poderes de governamentalidade[839].

Com base nisso, desenvolve junto a outros teóricos a chamada "Teoria Ator-Rede", segundo a qual humanos e não-humanos interagem entre si e influenciam-se mutuamente.[840] À época em que Latour desenvolveu sua teoria, já havia estudos explorando a forma pela qual a estrutura de conhecimento poderia ser analisada e interpretada através da interação entre atores e redes.

Neste sentido, podemos citar a obra de John Law e Peter Lodge, publicada em 1984, que foi elaborada como uma tentativa de entender processos de inovação e criação de conhecimento na ciência e na tecnologia. Dessa forma, essas teorias se opuseram à divisão formal binária entre homem e objeto, passando a afirmar que eles possuem a mesma importância e o mesmo conjunto de direitos[841]. Essa perspectiva acaba com os privilégios dos homens e põe fim às hierarquias, já que, ontologicamente, todos os seres estão no mesmo nível[842].[843]

Segundo Gustavo Amaral[844], a proposta teórica de Latour é que estendamos a historicidade dos seres humanos a todos os seres (incluindo os seres não-humanos). O que o antropólogo francês nos solicita é que deixemos de considerar apenas a história humana e passemos a considerar a história de todos

[838] REDAÇÃO. Bruno Latour: "O objetivo da ciência não é produzir verdade indiscutíveis, mas discutíveis". *Diálogos R7*, 11 mar. 2017. Disponível em: <http://www.correiodopovo.com.br/blogs/dialogos/2017/03/1005/bruno-latour-o-objetivo-da-ciencia-nao-e-produzir-verdade-indiscutiveis-mas-discutiveisblb/>. Acesso em: 07 ago. 2017.

[839] FOX, Nick J.; ALLDRED, Pam. New materialista social inquiry: designs, methods and the research-assemblage. *International Journal of Social Research Methodology*, v. 18, n. 4, p. 400, 2015.

[840] Cf. LAW, John; LODGE, Peter. *Science for Social Scientists*. London: Macmillan Press, 1984.

[841] LATOUR, Bruno. *A Esperança de Pandora*: Ensaios sobre a realidade dos estudos científicos. Trad.: Gilson Cesar Cardoso de Sousa. São Paulo: EDUSC, 2001, p. 169 e ss.

[842] AMARAL, Gustavo Rick. Uma dose de pragmatismo para as epistemologias contemporâneas: Latour e o parlamento das coisas. *Teccogs: Revista Digital de Tecnologias Cognitivas*, São Paulo, n. 12, p. 93, jul-dez. 2015.

[843] Na década de 1990, essa forma de estudo já se tornava popular e passou a ser utilizada por autores de outras áreas, como antropologia e estudos focados na crítica feminista. Nos anos 2000, a utilização da abordagem semiótica se expandiu, mas não há uma teoria ortodoxa a ser seguida pelos atores, que acabam adotando perspectivas substancialmente distintas.

[844] AMARAL, Gustavo Rick. Uma dose de pragmatismo para as epistemologias contemporâneas: Latour e o parlamento das coisas. *Teccogs: Revista Digital de Tecnologias Cognitivas*, São Paulo, n. 12, p. 106, jul-dez. 2015.

os seres como relevante. “O que Sartre disse dos humanos – que a existência deles precede a essência – deve ser dito de todos os actantes”.[845]

Uma das bases do pensamento de Latour se encontra na ideia do princípio da simetria[846], utilizado de forma generalizada para alcançar igualdade formal entre conceitos que foram historicamente definidos a partir de dicotomias, como humano/não-humano[847]. Segundo o autor, “na simetria entre humanos e não-humanos, mantenho constante a série de competências e propriedades que os agentes podem permutar sobrepondo-se um ao outro”[848].

Em outras palavras, Bruno Latour generaliza o princípio da simetria, de forma a desfazer o rigor binário e atribuir a seres não-humanos características humanas, concedendo condição histórica às coisas e também possibilitando sua atuação no campo político[849]. Adicione-se a isto, o fato de que a ação para Latour depende da associação de actantes[850], ou seja, não se resume a uma ação isolada pautada em uma propriedade humana. A ideia de atuação/agência é atribuída a todos os actantes pois esses estão “em processo de permutar competências, oferecendo um ao outro novas possibilidades, novos objetivos, novas funções”[851].

Essa troca de propriedades requer atenção. Um quebra-molas, como pontua Latour, é o resultado da mistura de vontades, histórias relacionadas a materiais de construção e cálculos matemáticos de engenheiros, legisladores, entre outros. Há uma troca de propriedades entre objetos e humanos, na qual

[845] LATOUR, Bruno. "Jamais fomos modernos", Crise, 1.ed, editora 34, 1994, 152p, trad.Carlos Irineu da Costa.
[846] O Princípio da simetria foi formulado por David Bloor no intuito de atacar o pressuposto de que fatores históricos, psicológicos e sociais não influenciariam o contexto da justificação, que seria uma construção lógica, racional e objetiva. O autor afirma que a sociologia deveria ser simétrica na sua explicação, isto é, os mesmos tipos de causa devem poder explicar crenças verdadeiras e falsas. BLOOR, David. *Knowledge and social imagery*. London: Routledge & Kegan Paul, 1976, p. 76; AMARAL, Gustavo Rick. Uma dose de pragmatismo para as epistemologias contemporâneas: Latour e o parlamento das coisas. *Teccogs: Revista Digital de Tecnologias Cognitivas*, São Paulo, n. 12, p. 96-97, jul-dez. 2015.
[847] AMARAL, Gustavo Rick. Uma dose de pragmatismo para as epistemologias contemporâneas: Latour e o parlamento das coisas. *Teccogs: Revista Digital de Tecnologias Cognitivas*, São Paulo, n. 12, p. 94, jul-dez. 2015.
[848] LATOUR, Bruno. *A Esperança de Pandora*: Ensaios sobre a realidade dos estudos científicos. Trad.: Gilson Cesar Cardoso de Sousa. São Paulo: EDUSC, 2001, p. 210
[849] AMARAL, Gustavo Rick. Uma dose de pragmatismo para as epistemologias contemporâneas: Latour e o parlamento das coisas. *Teccogs: Revista Digital de Tecnologias Cognitivas*, São Paulo, n. 12, pp. 105 e 108-109, jul-dez. 2015.
[850] Latour opta pelo termo “*actantes*” para englobar todos os agentes humanos e não-humanos, tendo em vista que o termo “ator” remete usualmente a agentes humanos.
[851] LATOUR, Bruno. 2001, op.cit., p. 210.

características de um tornam-se atributos de outro e vice-versa. Nas palavras de Latour: [852]

> A história que canto não é a história do *Homo faber,* em que o ousado inovador desafia as imposições da ordem social para fazer contato com uma matéria tosca e inumana, mas pelo menos objetiva. Procuro aproximar-me da zona onde algumas características da pavimentação (mas não todas) se tornam policiais e algumas características dos policiais (mas não todas) se tornam quebra-molas.

A Teoria Ator-Rede de Bruno Latour afirma que as visões tecnológicas e sociais estão equivocadas: deve-se abordar as duas perspectivas – tecnológica e social –, mas sem que uma prevaleça sobre a outra. Para a melhor compreensão da teoria, é preciso apresentar o que as palavras ator e rede exprimem. [853-854]. No que tange ao conceito de *ator*, Latour prefere deixá-lo de lado e adota a terminologia *actante*. Isso porque a palavra *ator* traria consigo um entendimento de que o termo se refere apenas aos humanos – o que não é o objetivo na sua teoria, que abarca tanto humanos como não-humanos. Sendo assim, o vocábulo *actante* representa a ideia de forma mais precisa [855], o que traz consequências até quanto à responsabilidade por atos que envolvam humanos e não-humanos: [856]

---

[852] Ibid, p. 218-219.

[853] Nas palavras do autor, "Percebemos agora que as técnicas não existem como tais e que nada há passível de ser definido, filosófica ou sociologicamente, como um objeto, um artefato ou um produto da tecnologia. Não existe, em tecnologia ou em ciência, nada capaz de servir de pano de fundo para a alma humana no cenário modernista. O substantivo "técnica" - e sua corruptela "tecnologia" - não precisam ser usados para separar os humanos dos múltiplos conjuntos com os quais eles combinam. Mas existe um *adjetivo,* "técnico", que podemos empregar adequadamente em muitas situações.". LATOUR, Bruno. *A Esperança de Pandora*: Ensaios sobre a realidade dos estudos científicos. Trad.: Gilson Cesar Cardoso de Sousa. São Paulo: EDUSC, 2001, p. 219.

[854] O autor, porém, não deixa de descrever o que considera como técnica: "A esta altura de nossa genealogia especulativa, não convém mais falar de humanos anatomicamente modernos, mas apenas de pré-humanos sociais. Enfim, estamos em condição de definir "técnica", no sentido de um *modus operandi*, com alguma precisão. As técnicas, ensinam-nos os arqueólogos, são subprogramas articulados para ações que subsistem (no tempo) e se estendem (no espaço). As técnicas não implicam sociedade (esse híbrido tardio), mas urna organização semi-social que arregimenta não-humanos de diferentes climas, lugares e materiais, Arco e flecha, lança, martelo, rede ou peça de vestuário são constituídos de partes e que exigem recombinação em sequência de tempo e sem relação com seus cenários originais. As técnicas são aquilo que acontece a ferramentas e atuantes não-humanos quando processados por urna organização que os extrai, recombina e socializa. Até as técnicas mais simples são sociotécnicas; até nesse nível primitivo de significado as formas de organização revelam-se inseparáveis dos gestos técnicos." LATOUR, Bruno. *A Esperança de Pandora*: Ensaios sobre a realidade dos estudos científicos. Trad.: Gilson Cesar Cardoso de Sousa. São Paulo: EDUSC, 2001, p. 240.

[855] Nas palavras do autor, "Uma vez que a palavra agente no caso dos não-humanos é incomum, um termo melhor é actant, um empréstimo de semiótica que descreve qualquer entidade que atua em uma trama até a atribuição de um papel figurativo ou não figurativo ("cidadão", "arma")". Tradução livre. No original: "Since the word agent in the case of nonhumans is uncommon, a better term is actant, a borrowing from semiotics that describes any entity that acts in a plot until

> Esses exemplos de simetria ator-actante nos força a abandonar a dicotomia sujeito-objeto, uma distinção que impede a compreensão das técnicas e até mesmo das sociedades. Não são nem as pessoas nem as armas que matam. A responsabilidade pela ação deve ser compartilhada entre os vários actantes.

Na concepção tradicional da agência moral, a tecnologia não pode ser considerada como agente moral "em si", e a alternativa é negar que a tecnologia é uma entidade moral. Concordando com a teoria e Latour, Peter Verbeek explica em maior detalhe a natureza exata do significado moral da tecnologia argumentando que a concepção tradicional da agência moral é falha e, portanto, é necessário repensar o conceito de agência moral.[857]

Verbeek argumenta que, uma vez que a ação humana é, na maioria dos casos, mediada e influenciada pela tecnologia, devemos considerar essa relação como um híbrido humano-tecnologia e são essas entidades híbridas que, em conjunto, podem ter uma agência moral. Podemos ver como isso faz sentido com referência ao exemplo anterior da arma. Em um entendimento tradicional da agência moral, o homem que decide matar seu chefe com uma arma é o agente, e ele faz a escolha de atirar em seu chefe com a arma, então ele se torna responsável. Mas como a arma é uma parte importante de sua decisão de atirar em seu chefe também: sem a arma, a escolha não poderia ter sido feita. Então, em certo sentido, a arma "ajuda" o homem a tomar a decisão também. O agente neste caso, de acordo com a agência híbrida da tecnologia humana de Verbeek, seria o homem e a arma, juntos, não apenas o próprio homem, e obviamente não a arma propriamente dita.[858]

Portanto, a definição de actante é obtida por meio do papel que ele possui na rede e os efeitos que gera a ela, podendo ser desde pessoas, animais, coisas, objetos até instituições, o que terá implicações no debate sobre responsabilidade e

---

the attribution of a figurative or non-figurative role ("citizen," weapon").'" LATOUR, Bruno. On Technical Meditation – Philosophy, Sociology, Genealogy. *Common Knowledge*, v. 3, n. 2, p. 33, 1994.

[856] Tradução livre. No original: "These examples of actor-actant symmetry force us to abandon the subject-object dichotomy, a distinction that prevents understanding of techniques and even of societies. It is neither people nor guns that kill. Responsibility for action must be shared among the various actants." LATOUR, Bruno. On Technical Meditation – Philosophy, Sociology, Genealogy. *Common Knowledge*, v. 3, n. 2, p. 34, 1994.

[857] VERBEEK, Peter. *Moralizing Technology:* Understanding and Designing the Morality of Things, Chicago - London, The University of Chicago Press. 2011.

[858] Ibid.

eticidade, que será abordado mais à frente. Já o conceito de rede, para Latour, representa as interligações de conexões onde os atores estão envolvidos. Segundo o antropólogo, a rede pode seguir para qualquer lado ou direção e estabelecer conexões com actantes que mostrem alguma similaridade ou relação.[859]

De acordo com a Teoria Ator-Rede, humanos e não-humanos são dotados de agência – possuem capacidade de atuar em sistemas ou redes – e devem ser tratados igualmente, uma vez que a separação entre esses elementos é de difícil concretização[860]. Assim, o que parece ser somente técnico, também é parcialmente social. O contrário também é verdadeiro.

Com o tempo, os objetos foram sendo aperfeiçoados até chegar num ponto em que estão presentes fisicamente e possuem uma importância emocional para os indivíduos. O aspecto fenomenológico, assim, incorpora o elemento material ao comportamento. Nesse sentido, por exemplo, ao assistir televisão, o indivíduo estaria ouvindo e vendo o próprio objeto, e não quem propaga as informações. Segundo Latour, tais objetos agem simbolicamente, conferindo significado, e nos dando o senso de aliança, no sentido de que podemos contar com eles para manter nosso sentimento de união, cria nas pessoas a ideia de pertencimento e similaridade e, por fim, estabiliza nossa vida através de rituais repetidos no dia a dia.

[859] LATOUR, Bruno. "*Jamais fomos modernos*", Crise, 1.ed, editora 34, 1994, 152p, trad.Carlos Irineu da Costa.

[860] "It is us, the human makers (so they say), that you see in those machines, those implements, us under another guise, our own hard work. *We should restore the human agency* (so they command) that stands behind those idols. We heard this story told, to different effect, by the NRA: Guns do not act on their own, only humans do so. A fine story, but too late. Humans are no longer by themselves. Our delegation of action to other actants that now share our human existences so far progressed that a program of antifetishism could only lead us to a nonhuman world, a world before the mediation of artifacts, a world of baboons". (negrito acrescentado) LATOUR, Bruno. On Technical Meditation – Philosophy, Sociology, Genealogy. *Common Knowledge*, v. 3, n. 2, p. 41, 1994. Confira-se versão traduzida para o português da obra "A Esperança de Pandora" em que trecho muito similar é reproduzido. Contudo, destacamos a versão americana pelo fato de o autor falar explicitamente em *agency*. "Ouvimos essa história contada, com outras intenções, pela NRA: as armas não agem sozinhas, apenas os humanos fazem isso. Boa história... mas que chegou séculos atrasada. Os humanos já não agem *por si mesmos.* A delegação de ação a outros atuantes, que agora compartilham nossa existência humana, foi tão longe que um programa de antifetichismo só nos arrastaria para um mundo não-humano, um fantasmagórico mundo perdido *anterior* à mediação dos artefatos. A erradicação da delegação pelos críticos antifetichistas tornaria o deslocamento *para baixo.* em direção aos artefatos técnicos, tão opaco quanto o deslocamento *para fora,* rumo aos fatos científicos". LATOUR, Bruno. *A Esperança de Pandora*: Ensaios sobre a realidade dos estudos científicos. Trad.: Gilson Cesar Cardoso de Sousa. São Paulo: EDUSC, 2001, p. 218.

A teoria ator-rede é, em suma, uma forma de mapear como as tecnologias, artefatos técnicos e objetos materiais participam do nosso cotidiano. A ideia de participar é importante, pois indica que os objetos estão agindo conosco. Ao distribuir agência a não-humanos e consolidar a ideia de simetria, a teoria nos traz uma contribuição enorme para pensarmos sobre o impacto que esses elementos vêm tendo em nossa sociedade.

Para melhor compreender esse fenômeno, exploraremos esse cenário envolvendo a capacidade de agência exercida por Coisas e algoritmos, analisando especificamente o impacto dos últimos na esfera pública conectada. Para isso, nos valeremos da perspectiva do chamado "novo materialismo" (em inglês, "*new materialism*"), baseada em grande medida nas contribuições teóricas de Bruno Latour.[861] Esse recorte teórico justifica-se por ser capaz de nos levar a uma melhor compreensão sobre o impacto de agentes não-humanos em nossa realidade social.

A ótica filosófica pós-humanista relacionada ao novo materialismo consolidou-se a partir da teoria crítica feminista que reconheceu a necessidade de uma nova lente teórica, crítica à perspectiva dualista. O novo materialismo, nesse contexto, desvencilha-se de concepções deterministas duais, que consideram a matéria como algo ontologicamente pré-determinado, para estabelecer uma teoria que valoriza a construção de sentido contínua e dinâmica, a partir de uma abordagem mais ampla do conceito de causalidade.[862] A perspectiva busca, assim, estabelecer uma ideia de "relacionalidade" entre sujeito e objeto, matéria e significado, humano e não-humano.

Iris van der Tuin e Rick Dolphijn assim explicam o termo "novo materialismo":[863]

> O novo materialismo é "novo", no sentido de que é uma tentativa de saltar para o futuro sem uma preparação adequada no presente, ao se tornar um movimento de "transformar-se em mais e transformar-se em outro", o que envolve a orientação para a criar o novo, um futuro desconhecido, que não é mais reconhecível em

[861] A corrente do novo materialismo, representanda por teóricos como Karen Barad, Jane Bennett, William Connolly, Diana Coole e Rosi Braidotti, foi fortemente influenciada pelos escritos de Donna Haraway (1991), autora do emblemático texto pós-humanista "O Manifesto Ciborgue", e de pós-estruturalistas como Bruno Latour (1993), M. Foucault e G. Deleuze.

[862] PARIKKA, Jussi; TIAINEN, Milla. *What is New Materialism*. Opening words from the event New Materialisms and Digital Culture. Anglia Ruskin University, 21-22 June 2010.

[863] Disponível em: <https://newmaterialistscartographies.wikispaces.com/New+Materialism>. Acesso em: 28 nov. 2017.

> termos do presente. Na arte, essa análise poderia ser o estudo da matéria e do significado.[864]

Nesse sentido, o pensamento feminista buscou afastar-se do pensamento que privilegia um padrão estabelecido, representado comumente pelo humano como homem branco, ocidental, heterossexual. Diferentemente, buscou incorporar no seu desenvolvimento outras concepções ontológicas sobre o humano. Esta nova perspectiva permite, para além da dualidade de gênero, um distanciamento também da posição que diferencia natureza e cultura, branco e negro, amigo e inimigo, baseada em uma separação estanque entre elementos que antes eram vistos como opostos.[865]

Segundo Nick Fox:[866]

> Uma nova ontologia materialista rompe com 'a mente e a cultura - divisões naturais do pensamento humanista transcendental' e também é, consequentemente, transversal a uma série de dualismos da teoria social, como estrutura/agência, razão/emoção, humano/não humano, animado/inanimado e dentro/fora. Fornece uma concepção de agência não vinculada à ação humana, deslocando o foco para a investigação social a partir de uma abordagem baseada em humanos e seus corpos, examinando, em vez disso, como redes relacionais ou reuniões de afetos animados e inanimados são afetados.[867]

O novo materialismo faz uma mescla entre natureza e cultura, considerando ambos esses elementos como parte de um entrelaçamento ("*entanglement*"). Segundo Karen Barad (2007) a matéria deve ser vista a partir de uma perspectiva relacional que apenas se constitui por meio das relações que estabelece com outros elementos. Observa-se, portanto, através desta lente pós-humanista, a existência de uma rede de relações, em interação com outros

---

[864] Tradução livre do autor. No original: *New materialism is then "new"in the sense that it is an attempt to 'leap into the future without adequate preparation in the present, through becoming, a movement of becoming-more and becoming-other, which involves the orientation to the creation of the new, to an unknown future, what is no longer recognizable in terms of the present.' In art this analysis could be the study of matter and meaning*.

[865] Disponível em: <http://www.tandfonline.com/doi/full/10.1080/13645579.2014.921458>. Acesso em: 19 set. 2017.

[866] FOX, Nick. *New materialist social inquiry:* designs, methods and the research-assemblage. 2014. Disponível em: <http://www.tandfonline.com/doi/full/10.1080/13645579.2014.921458>. Acesso em: 19 set. 2017.

[867] Tradução livre do autor. No original: *New materialist ontology breaks through 'the mind-matter and culture-nature divides of transcendental humanist thought' and is consequently also transversal to a range of social theory dualisms such as structure/agency, reason/emotion, human/non-human, animate/inanimate and inside/outside. It supplies a conception of agency not tied to human action, shifting the focus for social inquiry from an approach predicated upon humans and their bodies, examining instead how relational networks or assemblages of animate and inanimate affect and are affected.*

elementos, que são sempre potenciais.[868] Nesta perspectiva, o que "é" e o que sabemos sobre as coisas no mundo estão constantemente moldando um ao outro.

A ideia de relacionalidade passa a ser encarada como verdadeiro princípio metodológico utilizado para melhor compreender as relações entre matéria e discurso. A matéria deixa de ser compreendida como passiva ou inerte, ou como mero produto de discursos, e é vista como um fator ativo na construção dessas relações de entrelaçamentos dinâmicos entre humanos e não-humanos. É importante, portanto, verificar em primeiro lugar como se dão as relações entre esses elementos e como eles estão intra-relacionados.

Karen Barad é uma das principais teóricas do novo materialismo e busca inspiração nas ciências exatas, a partir das teorias de Niels Bohr, cujos trabalhos contribuíram decisivamente para a compreensão da estrutura atômica e da física quântica. Essa abordagem é combinada com uma visão feminista, pós-humanista e pós-estruturalista, formando as bases da concepção de "realismo agencial" da autora.

Há, no entanto, algumas diferenças em relação às outras correntes. Enquanto os pós-estruturalistas entendem e focam no fato de que a linguagem é fluida (com recorte teórico na própria problemática da linguagem), os novos materialistas apontam que a materialidade também não é estável. Esses conceitos são discutidos na obra de Barad "*Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*", publicada em 2007.[869] A ótica do novo materialismo busca ressignificar as categorias da subjetividade, da agência e da causalidade, visando uma melhor compreensão dos papéis que elementos humanos e não-humanos, materiais e discursivos, naturais e culturais desempenham nas práticas materiais sociais.[870]

Foucault em sua profícua produção científica, trabalha com a ideia de um "governo das coisas", em sua série de aulas sobre a governabilidade. Esse "governo das coisas" representa relações complexas entre coisas e pessoas, não constituindo, portanto, um conjunto de elementos separados da ideia do governo

[868] ARADAU, Claudia et al. *Discourse/materiality*. Critical security methods: New frameworks for analysis, p. 57-84, 2014.
[869] ARADAU, Claudia et al. *Discourse/materiality*. Critical security methods: New frameworks for analysis, p. 57-84, 2014.
[870] LEMKE, Thomas. *New Materialisms:* Foucault and the 'Government of Things'. Theory Culture & Society, april 2014.

dos humanos. Foucault afirma que "governar significa governar coisas". Em crítica à teoria Foucaltiana, Barad afirma que o materialismo tradicional de Michael Foucault negligenciou a importância dos elementos não-humanos em outras esferas.[871]

Segundo a concepção de Barad, "*Foucault's analysis remains one-sided and limited. It "focuses on the production of human bodies, to the exclusion of non-human bodies whose constitution he takes for granted*". Dessa forma, no seu conceito de agência, Foucault teria, segundo Barad, permanecido com a ideia de que coisas são passivas, e que apenas os humanos possuem a capacidade de agir. Portanto, não logrou, segundo a autora, analisar de forma adequada as relações complexas e dinâmicas que se estabelecem entre significado e matéria.[872]

Por outro ângulo, a noção de agência, segundo a perspectiva do novo materialismo, deve ser analisada por uma perspectiva multilateral. A falha na teoria de Foucault, segundo Barad, foi focar apenas nos fatores humanos para compreender determinadas circunstâncias. O que defende, de modo diverso, é introduzir uma leitura mais atenta aos efeitos que elementos não-humanos podem gerar. A ideia é identificar as formas com que a matéria é capaz de consolidar ou reorganizar relações de poder.[873]

Para isso, Barad fundamenta sua teoria no conceito de intra-ação. Intra-ações seriam os mecanismos por meio dos quais os seres e coisas se encontram em constante processo de definição, a partir das interações que estabelecem com o ambiente à sua volta.[874] A ideia de intra-ação como base para a construção de significado de um determinado elemento ajuda a compreender a nova formulação do conceito de agência. Ao invés de se considerarem os poderes de agência como atributos puramente humanos, entende-se que também fatores não-humanos podem gerar interferências (influências), capazes de conferir-lhes o status de 'agentes'. Intra-ação seria, então, a "constituição mútua de agências entrelaçadas [*entangled agencies*]"".[875]

---

[871] LEMKE, Thomas. *New Materialisms:* Foucault and the 'Government of Things'. Theory Culture & Society, april 2014..
[872] Ibid.
[873] FERNÁNDEZ, Maria. *Posthumanism*, New Materialism and Feminist Media Art
[874] BARAD, Karen. *Meeting the universe halfway:* Quantum physics and the entanglement of matter and meaning. duke university Press, 2007.
[875] Ibid.

Além disso, deixa-se de considerar agência como uma atuação unidirecional, com sujeito e objeto bem definidos, para estabelecer uma conexão baseada na ideia de relacionalidade entre todos os fatores na mesma rede sociotécnica.[876] Portanto, como dito anteriormente, a agência não é vista como algo dado (de forma determinística), mas sim como uma manifestação possível que se dá por meio dos processos de entrelaçamento ("*entanglement*").

Nesta ótica, não existe uma separação clara entre sujeito e objeto - entre aquele que realiza e sofre uma ação. O que há é uma relação de imbricação entre os elementos, que tanto afetam quanto são afetados uns pelos outros. Essa ideia dá origem a uma concepção dinâmica do significado das coisas. Os eventos passam, portanto, a ser percebidos como consequências de um jogo dinâmico entre diferentes agências.[877]

Essa percepção do novo materialismo é fortemente influenciada pelas teorias de Bruno Latour ao pensar as interações sociais a partir de uma ontologia de humanos e actantes não-humanos atuando em rede.[878] Em complemento à essa visão, Jane Bennet desenvolveu o conceito de "poder das coisas" (*thing power*) na obra "*Vibrant Matter: a political ecology of things*", publicada em 2010. O que a autora defende é que as coisas também têm de ser consideradas no processo político, que tem sido absolutamente dominado pela subjetividade humana.

É perceptível, portanto, o avanço que essas teorias representam em relação à teoria habermasiana, que não deve ser desconsiderada, mas complementada. Busca-se com isso uma melhor compreensão do atual cenário de maior interação com Coisas cada vez mais autônomas e influentes em nosso comportamento, produzindo impacto inclusive na esfera pública.

Reivindica-se, assim, uma perspectiva ética em sintonia com o entrelaçamento dos agentes humanos e não-humanos como parte de um movimento que percebe na condição contemporânea uma necessidade de superação de dualismos modernos como mente e corpo, natureza e sociedade, homem e máquina. O teórico Hans Jonas na obra "O princípio da

[876] PARIKKA, Jussi; TIAINEN, Milla. *What is New Materialism*. Opening words from the event New Materialisms and Digital Culture. Anglia Ruskin University, 21-22 June 2010.
[877] ARADAU, Claudia et al. *Discourse/materiality*. Critical security methods: New frameworks for analysis, p. 57-84, 2014.
[878] LATOUR, B. *Reassembling the Social:* an introduction to actor-network theory. Oxford University Press. 2005.

Responsabilidade" chama atenção, por exemplo, para a maneira como a dualidade homem versus coisa está entranhada em nossa cultura: "Toda ética tradicional é antropocêntrica. A entidade 'homem' e sua condição fundamental era considerada como constante quanto à sua essência, não sendo ela própria objeto da *techne* (arte; ofício) reconfiguradora".[879]

Em artigo recente, o sociólogo português Boaventura de Souza Santos defende o fim da perspectiva dualista para que consigamos avançar tanto na ontologia quanto na epistemologia. Nas palavras de Boaventura:[880]

> O dualismo natureza-sociedade, nos termos do qual a humanidade é algo totalmente independente da natureza e esta é igualmente independente da sociedade, é de tal maneira constitutivo da nossa maneira de pensar o mundo e a nossa presença e inserção no mundo que pensar de modo alternativo é quase impossível, por mais que o senso comum nos reitere que nada do que somos, pensamos ou fazemos pode deixar de conter em si natureza. Por que então a prevalência e quase evidência, no plano científico e filosófico, da separação total entre natureza e sociedade? Está hoje demonstrado que esta separação, por mais absurda, foi uma condição necessária da expansão do capitalismo. Sem tal concepção não teria sido possível conferir legitimidade aos princípios de exploração e de apropriação sem fim que nortearam a empresa capitalista desde o início. O dualismo continha um princípio de diferenciação hierárquica radical entre a superioridade da humanidade/sociedade e a inferioridade da natureza, uma diferenciação radical porque assente numa diferença constitutiva, ontológica, inscrita nos planos da criação divina. Isto permitiu que, por um lado, a natureza se transformasse num recurso natural incondicionalmente disponível para ser apropriado e explorado pelo homem para seu exclusivo benefício.
> (...)
> Tenho salientado que os três modos principais de dominação moderna –classe (capitalismo), raça (racismo) e sexo (patriarcado) – atuam articuladamente e que essa articulação varia com o contexto social, histórico e cultural. Mas não tenho dado atenção suficiente ao fato de este modo de dominação assentar-se na dualidade sociedade/natureza, e de tal modo que sem a superação desta dualidade nenhuma luta de libertação poderá ter êxito. Os filósofos, filósofas, cientistas sociais e humanistas devem colaborar com todos aqueles e aquelas que lutam contra a dominação no sentido de criar formas de compreensão do mundo que tornem possíveis práticas de transformação do mundo que libertem conjuntamente o mundo humano e o mundo não-humano.

Essa perspectiva é especialmente útil para a análise da conjuntura atual de IoT, em que o emprego de algoritmos é crescente nos mais variados campos - desde a interação nas redes sociais até robôs inteligentes. A sociedade contemporânea deve ser analisada a partir de uma perspectiva que considera a

[879] JONAS, Hans. *O princípio da responsabilidade: ensaio de uma ética para a civilização tecnológica*. Ed. Contraponto. Rio de Janeiro. 2015.
[880] SOUZA, BOAVENTURA. *A nova Tese Treza*. 2018. Disponível em: <http://outraspalavras.net/capa/boaventura-a-nova-tese-onze/>. Acesso em: 29 set. 2017.

agência como partindo de elementos tanto humanos quanto não-humanos, em processos de intra-ação que apenas se definem a partir das relações que estabelecem com o mundo. Todos esses elementos são capazes de gerar efeitos profundos sobre a sociedade atual. Segundo Law e Singleton, "humanos e não-humanos trabalham juntos para produzir efeitos".[881]

A produção de redes e associações surge da relação de mobilidade estabelecida entre os atores humanos e não humanos que se dá na convergência dos novos meios de sociabilidade que aparecem com a cultura digital, como por exemplo as redes sociais e as comunidades virtuais. As teorias apresentadas explicar que, na cultura contemporânea, actantes não-humanos (que podem ser um dispositivo inteligente, como computadores, smartphones, sensores, *wearables*, servidores, entre outros) e humanos agem mutuamente, interferem e influenciam o comportamento um do outro.[882] Nesse sentido, o não-humano pode ser encarado também como mediador, na medida em que ajuda a estabelecer a interação humana em todos os níveis sociais e media a relação destes com outros não-humanos.[883]

Nesse sentido, destaca-se trecho do Relatório sobre Ética e Algoritmos da Algorithms Watch:

> Uma pessoa que age de forma autônoma nunca é um ser absolutamente autônomo, mas existe em uma certa relação com o assunto em questão e com o contexto societário mais amplo; como tal, esta pessoa é - pelo menos, de acordo com percepções externas e padrões éticos – dependente desses fatores.[884]

Antes das contribuições pós-estruturalistas e pós-humanistas, a própria definição de atores e de agência impossibilitava que se considerasse o papel de objetos (Coisas) e algoritmos nesses conceitos. Se considerarmos que cada elemento capaz de gerar alterações no estado de coisas tem um papel, essa

---

[881] LAW, J. and SINGLETON, V. *Performing technologies' stories:* on social construtivism, performance, and performativity. Technology and Culture. 2000.

[882] LATOUR, Bruno. "*Jamais fomos modernos*", Crise, 1.ed, editora 34, 1994, 152p, trad.Carlos Irineu da Costa

[883] LEMOS, André. [2] *A comunicação das coisas:* teoria ator-rede e cibercultura]. São Paulo: Annablume, 2013.

[884] Tradução livre do autor. No original: *A person acting autonomously is never an absolutely autonomous being but rather exists in a certain relation to the matter at hand and to the wider societal context; as such, this person is – at least according to external perceptions and ethical standards – dependent on these factors.*

diferença faz com que se possa também considerar as "coisas" como atores e se pensar de forma mais arejada em regulação e responsabilidade dos agentes.[885]

Nesse sentido, para o pesquisador inglês Andrew Barry, o que é político o é em razão de associações. O autor defende que também materiais e tecnologias podem se tornar políticos, não apenas por serem usados para intermediar conflitos entre atores políticos, mas principalmente porque essas ferramentas estão imbricadas na estrutura humana e social.[886] Essa perspectiva se aproxima da ideia da teoria ator-rede desenvolvida por autores como Latour, Callon e John Law. Barry defende, em primeiro lugar, a prevalência do princípio da simetria generalizada: humanos e não-humanos teriam igual capacidade de influenciar as intenções de atores nas redes de associações. Essas associações se constituem da seguinte forma: um ator age; esse ato ocorre em relação a outros atos; juntos, esses atores produzem redes de atores vastas e imprevisíveis.

A teoria ator-rede de Bruno Latour, complementada pela filosofia do novo materialismo, é de fundamental importância para a compreensão dessas novas associações, enquadrando de forma mais adequada o panorama atual de avanço das coisas inteligentes cada vez mais autônomas e simbióticas às relações sociais. Sob essa ótica, podemos entender melhor o grau de influência que mecanismos não-humanos podem exercer sobre a vida em sociedade e a importância dos seus efeitos, inclusive sobre a esfera pública.

Com o desenvolvimento dessas novas tecnologias, novas categorias devem ser adotadas para entender as consequências de aplicação dessas ferramentas no cotidiano, bem como se deve atentar para o seu significativo poder de interferência nas relações humanas. É dessa forma que o pós-humanismo e o pós-estruturalismo nos ajudam a compreender as novas características da contemporaneidade, considerando os poderes de agência desses elementos não-humanos, e fornecendo meios para interpretar a sua atuação.

Essas teorias, no entanto, não possuem o condão de analisar a rede e os actantes do ponto de vista jurídico ou regulatório. Por isso, apesar de ser uma

[885] LATOUR, Bruno. *Reassembling the social.* Hampshire: Oxford University Press, 2007.
[886] BARRY, A. (2001). *Political Machines:* Governing a Technological Society. London: Athlone Press.

instância crucial para o desenvolvimento teórico que pretendemos defender nesse estudo, é necessário irmos além destas.

Almejando, portanto, uma perspectiva regulatória destes fenômenos, entende-se como importante aplicarmos as correntes éticas aqui levantadas à luz da governança de algoritmos e da complexidade de novos artefatos técnicos e sistemas sociotécnicos, buscando endereçar questões de atribuição de responsabilidade e dever moral de actantes, conforme veremos a seguir.

3.4
Ética das Coisas e Governança de Algoritmos em Artefatos e Sistemas Sociotécnicos

"By ratiocination, I mean computation" [887]

(Thomas Hobbes, **1655**)

A partir dos anos 1980, com o progressivo desenvolvimento de computadores nos negócios e na administração pública, houve a percepção de que as práticas governamentais e corporativas ao processar dados pessoais estavam reduzindo os indivíduos a meros dados, ameaçando seus direitos fundamentais e sua liberdade. Atualmente, tal cenário continua o mesmo, sendo diferente apenas na ubiquidade e no aumento de poder dos meios tecnológicos de informação e de comunicação[888].

[887] THOMAS HOBBES, ELEMENTS OF PHILOSOPHY (1655), reprinted in 1 THE ENGLISH WORKS OF THOMAS HOBBES 1, 3 (William Molesworth ed., London, J. Bohn 1839); see also THOMAS HOBBES, LEVIATHAN (1670), reprinted in 3 THE ENGLISH WORKS OF THOMAS HoBBES 1, supra, at 29-32 [hereinafter LEVIATHAN] (equating reason with computation or "reckoning of the consequences"). Hobbes uses "ratiocination" to mean reasoning. *In: Carolyn P. et al. The Cognitive Sciences: An Interdisciplinary Approach. Sage, 2013. Disponível em: <http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=3447&context=nclr>. Acesso em: 29 set. 2017.*

[888] EUROPEAN DATA PROTECTION SUPERVISOR. *Towards a new digital ethics:* data, dignity and technology, 2015, p. 6. Disponível em: <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf>. Acesso em: 16 fev. 2017.

Em uma escala ainda maior, essa é a tese reforçada pelo escritor israelense Yuval Noah Harari[889] ao tratar da perda de liberdade humana e do que denomina de a nova religião dos dados:[890]

> Pensadores humanistas como Rousseau nos convenceram de que nossos próprios sentimentos e desejos eram a fonte suprema de significado, e que o nosso livre arbítrio era, portanto, a máxima autoridade. Agora, uma nova mudança está ocorrendo. Assim como a autoridade divina foi legitimada por mitologias religiosas, e a autoridade humana foi legitimada por ideologias humanistas, os gurus *high-tech* e os profetas do Vale do Silício estão criando uma nova narrativa universal que legitima a autoridade de algoritmos e *Big Data*. Esta crença romanceada pode ser chamada de "Dataísmo". Em sua forma extrema, os defensores da visão de mundo Dataísta percebem todo o universo como um fluxo de dados, vêem nos organismos algo como algoritmos bioquímicos, e acreditam que a vocação cósmica da humanidade é criar um sistema de processamento de dados abrangente - e depois fundir-se a isto. Já estamos nos tornando pequenos chips dentro de um sistema gigante que ninguém realmente entende. Todos os dias absorvo inúmeros bits de dados através de e-mails, telefonemas e artigos, processo os dados e transmito de volta novos bits através de mais e-mails, telefonemas e artigos. Eu realmente não sei onde me encaixo no grande esquema das coisas e como meus bits de dados se conectam com os bits produzidos por bilhões de outros seres humanos e computadores. Eu não tenho tempo para descobrir, porque estou muito ocupado respondendo e-mails. Este fluxo de dados implacável provoca novas invenções e interrupções que ninguém planeja, controla ou compreende.[891]

---

[889] Harari argumenta em sua obra Homo Deus que estamos caminhando para um mundo pós antropocêntrico, onde o valor da realidade é extraído a partir de constantes processamentos de informação, realizados por agentes humanos e não-humanos. Em um sentido similar, Luciano Floridi sustenta: "I*CTs are bringing about a fourth revolution, in the long process of reassessment of humanity's fundamental nature and role in the universe. We are not immobile, at the centre of the universe (Copernican revolution); we are not unnaturally distinct and different from the rest of the animal world (Darwinian revolution); and we are far from being entirely transparent to ourselves (Freudian revolution). ICTs are now making us realise that we are not disconnected agents, but informational organisms (inforgs), who share with other kinds of agents a global environment, ultimately made of information, the infosphere (Turing revolution).*" Disponível em: http://www.philosophyofinformation.net/books/the-fourth-revolution-how-the-infosphere-is-reshaping-human-reality/>. Acesso em 27 nov. 2017.

[890] Disponível em: <https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c>. Acesso em 27 nov. 2017.

[891] Tradução livre do autor. No original: *Humanist thinkers such as Rousseau convinced us that our own feelings and desires were the ultimate source of meaning, and that our free will was, therefore, the highest authority of all. Now, a fresh shift is taking place. Just as divine authority was legitimised by religious mythologies, and human authority was legitimised by humanist ideologies, so high-tech gurus and Silicon Valley prophets are creating a new universal narrative that legitimises the authority of algorithms and Big Data. This novel creed may be called "Dataism". In its extreme form, proponents of the Dataist worldview perceive the entire universe as a flow of data, see organisms as little more than biochemical algorithms and believe that humanity's cosmic vocation is to create an all-encompassing data-processing system — and then merge into it. We are already becoming tiny chips inside a giant system that nobody really understands. Every day I absorb countless data bits through emails, phone calls and articles; process the data; and transmit back new bits through more emails, phone calls and articles. I don't*

> (…)
> Embora os humanistas tenham errado em pensar que nossos sentimentos refletiram um "livre arbítrio" misterioso, até agora o humanismo ainda fazia um bom senso prático. Pois, embora não houvesse nada mágico em relação aos nossos sentimentos, eles foram, no entanto, o melhor método do universo para tomar decisões - e nenhum sistema externo poderia entender meus sentimentos melhor do que eu. (…) Isto é apenas o começo. Dispositivos como o Kindle da Amazon podem coletar constantemente dados de seus usuários enquanto estes estão lendo livros. Seu Kindle pode monitorar quais partes de um livro você lê rapidamente e quais lê lentamente; Em qual página você deu uma pausa, e em qual frase você abandonou o livro, para nunca mais o ler. Se o Kindle fosse atualizado com software de reconhecimento facial e sensores biométricos, saberia como cada frase influenciava sua freqüência cardíaca e pressão arterial. Saberia o que fez você rir, o que o deixou triste e o que o deixou com raiva. Em breve, os livros vão te ler enquanto você está lendo. E, enquanto você rapidamente esquece a maioria do que lê, programas de computador nunca devem esquecer. Esses dados devem eventualmente permitir que a Amazon escolha livros para você com uma inquietante precisão. Também permitirá que a Amazon saiba exatamente quem você é, e como apertar seus botões emocionais.[892]

Com a crescente difusão do *Big Data* e de técnicas de computação, a evolução tecnológica e a pressão econômica se espalharam rapidamente e os algoritmos se tornaram um ótimo recurso para inovação e para modelos de negócios. Esta rápida difusão dos algoritmos e sua crescente influência, porém, trazem consequências para o mercado e para a sociedade, o que inclui questões de ética e de governança[893].

---

really know where I fit into the great scheme of things, and how my bits of data connect with the bits produced by billions of other humans and computers. I don't have time to find out, because I am too busy answering emails. This relentless dataflow sparks new inventions and disruptions that nobody plans, controls or comprehends.

[892] Tradução livre do autor. No original: *Even though humanists were wrong to think that our feelings reflected some mysterious "free will", up until now humanism still made very good practical sense. For although there was nothing magical about our feelings, they were nevertheless the best method in the universe for making decisions — and no outside system could hope to understand my feelings better than me. (...) This is just the beginning. Devices such as Amazon's Kindle are able constantly to collect data on their users while they are reading books. Your Kindle can monitor which parts of a book you read quickly, and which slowly; on which page you took a break, and on which sentence you abandoned the book, never to pick it up again. If Kindle was to be upgraded with face recognition software and biometric sensors, it would know how each sentence influenced your heart rate and blood pressure. It would know what made you laugh, what made you sad, what made you angry. Soon, books will read you while you are reading them. And whereas you quickly forget most of what you read, computer programs need never forget. Such data should eventually enable Amazon to choose books for you with uncanny precision. It will also allow Amazon to know exactly who you are, and how to press your emotional buttons.*

[893] SAURWEIN, Florian; JUST, Natascha; LATZER, Michael. *Governance of algorithms:* options and limitations. Info, v. 17, n. 6, p. 35-49, 2015.

Tendo em vista que os algoritmos têm a capacidade de penetrar em inúmeros ramos de nossas vidas (inclusive colonizando o mundo da vida, conforme sustentado nesse trabalho) conforme se tornam mais sofisticados, úteis e autônomos, há o risco de que eles tomem decisões importantes no lugar de seres humanos[894]. Diante disto, Danilo Doneda e Virgilio Almeida defendem que para fomentar a integração dos algoritmos em processos sociais e econômicos são necessários instrumentos de governança dos algoritmos[895].

A governança de algoritmos [896] pode variar entre o ponto de vista estritamente legal e regulatório e o ponto de vista puramente técnico. Isto depende de alguns fatores, como a natureza do algoritmo, o contexto ou seus riscos[897]. Pode ocorrer, como visto, em múltiplos níveis, soluções orientadas ao mercado ou mecanismos governamentais de base. No primeiro caso, há a possibilidade de haver, por exemplo, regulação por companhias privadas, por meio da organização interna, e autorregulação de toda a indústria. Em ambos os casos, os *standards* adotados devem se basear no interesse público. Já no caso da regulação governamental, foca-se em requisitos como o nível de transparência ou de qualidade do serviço[898].

Dentre os pontos de regulação, se encontram a transparência, a responsabilidade – que se liga às noções de justiça e devido processo – e garantias técnicas, além do desenvolvimento de princípios éticos relativos ao uso de dados pessoais (*Big Data Ethics*). Destaque-se, que os algoritmos estão trabalhando

[894] Como observa Nicholas Diakopoulos, "We are now living in a world where algorithms, and the data that feed them, adjudicate a large array of decisions in our lives: not just search engines and personalized online news systems, but educational evaluations, the operation of markets and political campaigns, the design of urban public spaces, and even how social services like welfare and public safety are managed." (DIAKOPOULOS, Nicholas. Algorithm Accountability – Journalistic investigation of computational power structures. *Digital Journalism*, v. 3, n. 3, p. 398, 2015).

[895] DONEDA, Danilo; ALMEIDA, Virgilio A. F. What Is Algorithm Governance? *IEEE Internet Computing*, v. 20, p. 60, 2016.

[896] Dentre as opções de governança, que possuem suas limitações e são influenciadas por fatores contextuais, como incentivos e conflitos de interesse, temos as seguintes: (i) auto-organização de companhias individuais; (ii) autorregulação coletiva; (iii) corregulação e (iv) intervenção estatal. SAURWEIN, Florian; JUST, Natascha; LATZER, Michael. Governance of algorithms: options and limitations. *Info*, v. 17, n. 6, p. 38-43, 2015.

[897] DONEDA, Danilo; ALMEIDA, Virgilio A. F. What Is Algorithm Governance? *IEEE Internet Computing*, v. 20, p. 61, 2016.

[898] Ibid, p. 62.

constantemente e enfrentam situações não previstas e sem precedentes com frequência, de modo que seu monitoramento deve ser constante[899].

Um dos principais temas levantados pela doutrina quando se fala de governança consiste na opacidade dos algoritmos. O problema da opacidade se relaciona à dificuldade de decodificar o resultado gerado pelo algoritmo. Isto porque a inabilidade humana para decodificar o resultado de algoritmos pode criar problemas quando eles são usados para tomar decisões importantes que afetem nossas vidas. Assim, tem se falado na necessidade de haver maior transparência, o que poderia ser obtido por meio da regulação[900].

Segundo Relatório elaborado por grandes nomes do ramo de Ética Digital como Luciano Floridi e Wendell Wallach:[901]

> A inescrutabilidade ou transparência significativa pode prejudicar a aceitabilidade dos sistemas de implantação em situações nas quais podem ocorrer danos às pessoas, animais, meio ambiente ou instituições. Se o sistema falhar e causar danos, torna-se fundamental ter uma capacidade forense que garanta que acidentes ou falhas semelhantes não ocorram, e para determinar prestação de contas e responsabilização. Isto é especialmente importante quando os resultados são inesperados e / ou não estão alinhados com a intenção original para a qual o sistema foi implantado.[902]

Sobre esse problema, aprofundam o debate os pesquisadores do Oxford Internet Institute e Alan Turing Institute:[903]

> Os principais componentes da transparência são a acessibilidade e a compreensão da informação. Informações sobre a funcionalidade dos algoritmos geralmente são pouco acessíveis, intencionalmente. Algoritmos proprietários são mantidos em segredo por causa da vantagem competitiva, segurança nacional ou privacidade. A transparência pode, por consequência, contrariar outros ideais éticos, em particular a privacidade dos titulares de dados e a autonomia das organizações. (...) A viabilidade comercial dos processadores de dados em muitas

---

[899] Ibid.
[900] DONEDA, Danilo; ALMEIDA, Virgilio A. F. op.cit, p. 60-62, 2016.
[901] WALLACH, Wendell, et al. *Artificial Intelligencefor the Common Good Sustainable*, Inclusive and Trustworthy. 2017. Disponível em: <https://weforum.ent.box.com/v/AI4Good?platform=hootsuite>. Acesso em: 28 fev. 2017.
[902] Tradução livre do autor. No original: *A lack of scrutability or meaningful transparency can undermine the acceptability of deploying systems in situations where harm may occur to people, animals, the environment or institutions. Should the system fail and cause harm, it becomes critical to have a forensic capability to ensure similar accidents or failures do not occur, and to determine accountability and liability. This is especially important when outcomes are unexpected and/or not aligned with the original intent for which the system was deployed.*
[903] MITTELSTADT, Brent, et al. *The ethics of algorithms:* Mapping the debate. Big Data & Society July–December 2016.

> indústrias pode estar ameaçada pela transparência. No entanto, os titulares de dados têm interesse em entender como suas informações são criadas e influenciam as decisões tomadas nas práticas de dados orientados. Esta luta é marcada pela assimetria de informação e um "desequilíbrio no conhecimento e poder de decisão", que favorece os processadores de dados. Além de ser acessível, a informação deve ser compreensível para ser considerada transparente. Os esforços para tornar os algoritmos transparentes enfrentam um desafio significativo, à medida que precisam transformar processos complexos de tomada de decisão em algo acessível e compreensível. O problema, à longo prazo, da interpretação em algoritmos de *machine learning* indica o desafio da opacidade em algoritmos. (...) A divulgação de transparência por parte dos processadores e controladores de dados pode revelar-se crucial no futuro, para manter um relacionamento confiável com os titulares de dados.[904]

Sobre a necessidade de maior transparência, vale dizer que recentemente a cidade de Nova York aprovou por unanimidade um projeto de lei voltado às agências governamentais que usam algoritmos para auxiliar em processos judiciais. Visto como um projeto de lei de responsabilidade algorítmica, o primeiro do tipo na regulação legislativa norte-americana, a norma estabelecerá uma força-tarefa para estudar como os algoritmos estão sendo usados pelas agências da cidade para tomar decisões que afetam os cidadãos de Nova York. A força-tarefa concentrará em grande parte seus esforços na investigação do viés algorítmico e se qualquer um dos modelos é discriminatório contra pessoas com base na idade, raça, religião, gênero, orientação sexual ou status de cidadania.[905]

À exemplo da nova regulação norte-americana que visa jogar luz sobre os algoritmos evitando seu tratamento como "caixas pretas", é importante frisar que as empresas e organizações governamentais devem procurar reduzir o viés algorítmico e fornecer a maior transparência possível aos modelos preditivos.

---

[904] Tradução livre do autor. No original: *The primary components of transparency are accessibility and comprehensibility of information. Information about the functionality of algorithms is often intentionally poorly accessible. Proprietary algorithms are kept secret for the sake of competitive advantage, national security, or privacy. Transparency can thus run counter to other ethical ideals, in particular the privacy of data subjects and autonomy of organisations. (...) The commercial viability of data processors in many industries may be threatened by transparency. However, data subjects retain an interest in understanding how information about them is created and influences decisions taken in datadriven practices. This struggle is marked by information asymmetry and an ‘‘imbalance in knowledge and decision-making power’’ favouring data processors. Besides being accessible, information must be comprehensible to be considered transparent. Efforts to make algorithms transparent face a significant challenge to render complex decisionmaking processes both accessible and comprehensible. The longstanding problem of interpretability in machine learning algorithms indicates the challenge of opacity in algorithms.(...) Transparency disclosuresby data processors and controllers may prove crucial in the future to maintain a trusting relationship with data subjects.*

[905] Disponível em: <http://www.businessinsider.com/algorithmic-bias-accountability-bill-passes-in-new-york-city-2017-12>. Acesso em: 28 nov. 2017.

Na europa, A GDPR (General Data Protection Regulation), mencionada anteriormente neste trabalho, prevê o direito de obter uma explicação para qualquer decisão feita por um algoritmo e também o direito de optar pela não-coleta de dados. Muitos sugerem que esse padrão é muito amplo e terá que ser revisado. No entanto, está funcionando como uma ferramenta para responsabilizar as partes interessadas. Além disso, motivou os engenheiros a explorar os meios para fornecer pelo menos um grau de transparência maior sobre como os algoritmos com *machine learning* tomam suas decisões.

Em complemento, o cientista principal de AI da Google, John Giannandrea, destaca os riscos de sistemas inescrutáveis:[906]

> É importante que possamos ser transparentes sobre os dados de treinamento que estamos usando, e estamos procurando por vieses ocultos, senão estaremos construindo sistemas tendenciosos (...) se alguém tenta vender um sistema de caixa preta que sustente decisões médicas, e você não sabe como ela funciona ou quais dados foram usados para treiná-la, então não confiaria nisso.[907]

Pesquisadores da Universidade de Zurique[908] afirmam que a governança de algoritmos deve ser feita com base em ameaças identificadas e propõem uma *abordagem baseada no risco*, destacando aqueles relacionados a manipulação, preconceitos, censura, discriminação social, violações de privacidade, direitos de propriedade e abuso do poder de mercado[909]. Para evitar que estes riscos se concretizem, é necessário recorrer à governança.

Além da tecnologia dos algoritmos em si, outros fatores externos influenciam o seu desenvolvimento e a necessidade de sua regulação. É o caso das bases de dados. Os algoritmos tornam-se mais úteis à medida em que há mais dados disponíveis[910]. Se os dados são algo fundamental para os algoritmos, que

---

[906] KNIGHT, Will. "*Forget Killer Robots...",* MIT Technology Review, Disponível em: <https://www.technologyreview.com/s/608986/forget-killer-robotsbias-is-the-real-ai-danger/>. Acesso em: 28 nov. 2017.

[907] Tradução livre do autor. No original: *It's important that we be transparent about the training data that we are using, and are looking for hidden biases in it, otherwise we are building biased systems (...) if someone is trying to sell you a black box system for medical decision support, and you don't know how it works or what data was used to train it, then I wouldn't trust it.*

[908] SAURWEIN, Florian; JUST, Natascha; LATZER, Michael. Governance of algorithms: options and limitations. *Info*, v. 17, n. 6, p. 37 e ss., 2015.

[909] Ibid.

[910] DONEDA, Danilo; ALMEIDA, Virgilio A. F. What Is Algorithm Governance? *IEEE Internet Computing*, v. 20, p. 61, 2016.

são inertes até que pareados com bases de dados[911], é preciso analisar o tratamento legal dado a eles, pois devem ser legítimos, corretos, atualizados e não baseados em preconceitos. Isto porque métodos de lidar com os dados podem gerar discriminação e resultados tendenciosos, por exemplo, o que ressalta a necessidade de existir uma lei geral de proteção a dados pessoais, aqui defendida.

Com base nisso, há técnicas de governança dos algoritmos que não atuam diretamente sobre os algoritmos em si, mas nos dados que os alimentam. Como observam Danilo Doneda e Virgilio Almeida:[912][913]

> É verdade que há várias ferramentas já presentes na legislação de proteção de dados de alguns países, que possuem medidas de transparência e equidade aplicadas diretamente a algoritmos e plataformas que suportam seu funcionamento. Por exemplo, a disposição de que as decisões automatizadas devem basear-se em critérios transparentes está comumente presente em várias leis de proteção de dados. O mesmo acontece com o direito de solicitar uma revisão humana das decisões tomadas automaticamente.[914]

Com a análise de opções e limitações acerca da governança, pesquisadores da Universidade de Zurique concluem que não há uma solução que sirva para todos os casos, mas deve haver um misto entre governança e respeito a cada ator envolvido:[915]

---

[911] GILLESPIE, Tarleton. The Relevance of Algorithms. In: _____; BOCZKOWSKI, Pablo J.; FOOT, Kirsten A. (Eds.). Media Technologies: Essays on Communication, Materiality, and Society. *Cambridge (MA):* The MIT Press, 2014, p. 169. O autor nota que a análise de algoritmos deve estar sempre ligada à análise de dados: "Algorithms are inert, meaningless machines until paired with databases on which to function. A sociological inquiry into an algorithm must always grapple with the databases to which it is wedded; failing to do so would be akin to studying what was said at a public protest, while failing to notice that some speakers had been stopped at the park gates.".

[912] DONEDA, Danilo; ALMEIDA, Virgilio A. F. What Is Algorithm Governance? IEEE Internet Computing, v. 20.

[913] Tradução livre do autor. No original: *This is true for several tools already present in dataprotection legislation that, in some countries, have measures regarding transparency and fairness that apply directly to algorithms and the platforms that support their functioning. For instance, the provision that automated decisions shall be grounded on transparent criteria is commonly present in several pieces of data-protection legislation. The same happens with the right to ask for a human revision of automatically taken decisions.*

[914] Tradução livre do autor: Isso é verdade para várias ferramentas já presentes na legislação de proteção de dados que, em alguns países, possuem medidas de transparência e equidade que se aplicam diretamente a algoritmos e plataformas que suportam seu funcionamento. Por exemplo, a disposição de que as decisões automatizadas devem basear-se em critérios transparentes está comumente presente em várias leis de proteção de dados. O mesmo acontece com o direito de solicitar uma revisão humana das decisões tomadas automaticamente.

[915] Tradução livre do autor. No original: *Analyses reveal that there is a broad spectrum of players, levels and instruments for the governance of algorithms, but there is no one-size-fits-all solution. Instead, there is the need for a governance mix consistent with the respective risks and applications in question and an interplay between instruments and diverse actors involved. The*

> Análises revelam que há um amplo espectro de jogadores, níveis e instrumentos para a governança de algoritmos, mas não existe uma solução única para tudo. Em vez disso, existe a necessidade de um mix consistente de governança com os respectivos riscos e aplicações em questão, e uma interação entre instrumentos e os diversos atores envolvidos. A atenção, portanto, deve mudar para soluções multidimensionais e combinações de medidas de governança que se permitem e complementam mutuamente. (...) A busca de um mix adequado de governança é difícil porque há apenas conhecimentos limitados sobre o desenvolvimento e efeitos das intervenções regulatórias. As incertezas existentes exigem maior avaliação de risco e tecnologia para fortalecer as bases para a governança baseada em evidências no domínio da seleção algorítmica. As abordagens baseadas em risco parecem ser apropriadas para esse fim. Podem monitorar o desenvolvimento de mercado e tecnologia, avaliar riscos envolvidos ou emergentes e desenvolver estratégias adaptáveis de governança para os problemas.[916][917]

Já Lucas Introna[918], professor da Universidade de Lancaster, considera que a melhor solução não seja a governança, mas a governamentalidade. Para o autor, as próprias práticas de governança deveriam ser governadas, pois elas nunca são seguras enquanto tais. A governamentalidade, vista portanto, como uma meta-governança, consideraria a natureza performativa das práticas de governança (e seus resultados) e permitiria mostrar a natureza constitutiva mútua de problemas, domínios de conhecimento e subjetividades comandadas por práticas de governo. Ligadas às tecnologias de governo, estariam as práticas de cálculo (*calculative practices*), que constituem domínios de conhecimento e expertise. Tais práticas

---

attention therefore has to shift to multi-dimensional solutions and combinations of governance measures that mutually enable and complement each other. (...) The search for an adequate governance mix is difficult because there is only limited knowledge about the development and the effects of regulatory interventions. The existing uncertainties call for further risk and technology assessment to strengthen the foundations for evidence-based governance in the domain of algorithmic selection. Risk-based approaches seem to be particularly appropriate for this purpose. They can monitor market and technology developments, assess the involved and emerging risks and develop problem-oriented, adaptive governance strategies.

[916] SAURWEIN, Florian; JUST, Natascha; LATZER, Michael. *Governance of algorithms:* options and limitations. Info, v. 17, n. 6, p. 44, 2015.

[917] Tradução livre do autor: As análises revelam que há um amplo espectro de jogadores, níveis e instrumentos para a governança de algoritmos, mas não existe uma solução de tamanho único. Em vez disso, existe a necessidade de um mix de governança consistente com os respectivos riscos e aplicações em questão e uma interação entre instrumentos e diversos atores envolvidos. A atenção, portanto, deve mudar para soluções multidimensionais e combinações de medidas de governança que se permitem e complementam mutuamente. (...) A busca de um mix de governança adequado é difícil porque há apenas conhecimentos limitados sobre o desenvolvimento e os efeitos das intervenções regulatórias. As incertezas existentes exigem maior avaliação de risco e tecnologia para fortalecer as bases para a governança baseada em evidências no domínio da seleção algorítmica. As abordagens baseadas em risco parecem ser particularmente apropriadas para esse fim. Eles podem monitorar os desenvolvimentos de mercado e tecnologia, avaliar os riscos envolvidos e emergentes e desenvolver estratégias de governança adaptativa orientadas para o problema.

[918] INTRONA, Lucas D. Algorithms, Governance, and Governmentality*:* On Governing Academic Writing. *Science, Technology, & Human Values*, v. 41, n. 1, p. 17-49, 2016.

contém certa autoridade moral, pois impõem neutralidade e objetividade a um domínio que possui relevância moral (o autor exemplifica com um algoritmo criado para identificar o plágio). Com base nisto, o professor conclui:[919]

> Assim, a compreensão das práticas governamentais no idioma da governabilidade nos permite ver como os problemas, as tecnologias de governança, os regimes de conhecimento e as subjetividades se tornam mutuamente constitutivos uns dos outros para criar um regime de governo que não tem essência específica (localização ou ação unificada). Todos os resultados performativos "nunca [são] simplesmente a realização de um programa, estratégia ou intenção: enquanto a vontade de governar os atravessa, eles não são simplesmente realizações de qualquer vontade simples.[920]

Com outro enfoque, ao tratar sobre a responsabilidade relacionada aos algoritmos, Nicholas Diakopoulos afirma que o ponto crucial é a tomada de decisão autônoma, uma vez que as decisões feitas por algoritmos podem ser baseadas em heurísticas[921]:[922]

> Decisões algorítmicas podem basear-se em heurísticas e regras, ou em cálculos sobre quantidades maciças de dados. As regras podem ser articuladas diretamente pelos programadores, ou ser dinâmicas e flexíveis com base em dados *machine learning*. Às vezes, um operador humano mantém a agência e toma a decisão final em um processo, mas mesmo neste caso, o algoritmo inclina a atenção do operador para um subconjunto de informações.[923]

Dentro dessa lógica de resultados com base em preconceitos, é importante, também, destacar que os algoritmos são programados para classificar os dados que lhes são enviados e, muitas vezes, erros podem ser cometidos, podendo haver falsos positivos e falsos negativos. Como exemplifica Diakopoulos[924], o YouTube

---

[919] Tradução livre do autor. No original: *Thus, understanding governing practices in the idiom of governmentality allows us to see how problems, technologies of governance, regimes of knowledge, and subjectivities become mutually constitutive of each other to create a regime of government that has no specific essence (location or unified action). All the performative outcomes are 'never simply a realization of a programme, strategy or intention: whilst the will to govern traverses them, they are not simply realizations of any simple will'.*

[920] INTRONA, Lucas D. Algorithms, Governance, and Governmentality: On Governing Academic Writing. *Science, Technology, & Human Values*, v. 41, n. 1, p. 39, 2016.

[921] Heurística é um método ou processo criado com o objetivo de encontrar soluções para um problema.

[922] Tradução livre do autor. No original: *Algorithmic decisions can be based on heuristics and rules, or calculations over massive amounts of data. Rules may be articulated directly by programmers, or be dynamic and flexible based on machine learning of data. Sometimes a human operator maintains agency and makes the final decision in a process, but even in this case the algorithm biases the operator's attention toward a subset of information.*

[923] DIAKOPOULOS, Nicholas. Algorithm Accountability – Journalistic investigation of computational power structures. *Digital Journalism*, v. 3, n. 3, p. 400, 2015.

[924] DIAKOPOULOS, Nicholas, 2015. op.cit p. 401.

classifica os vídeos enviados ao site de acordo com as músicas que são reproduzidas a fim de verificar se há infração a direitos autorais. Um falso positivo, nesse caso, seria um vídeo classificado como infrator, mas que, na verdade, se enquadra numa hipótese de *fair use*. Um falso negativo, por sua vez, seria um vídeo classificado como *fair use*, mas que, na prática, violou direitos autorais.

Considerando que os algoritmos exercem poder por si próprios, mas são sempre influenciados por seres humanos que os criaram, Diakopoulos afirma que a responsabilidade deve considerar a intenção dos criadores do algoritmo, o processo que influenciou seu design e, ainda, a agência que interpreta os resultados gerados[925]. Confira-se, ainda, os ensinamentos de Nick Bostrom, filósofo da Universidade de Oxford, e Eliezer Yudkowsky, cofundador do *Machine Intelligence Research Institute*:

> Outro importante critério social para transações em organizações é ser capaz de encontrar a pessoa responsável por conseguir que algo seja feito. Quando um sistema de IA falha em suas tarefas designadas, quem leva a culpa? Os programadores? Os usuários finais? Burocratas modernos muitas vezes se refugiam nos procedimentos estabelecidos que distribuem responsabilidade amplamente, de modo que uma pessoa não pode ser identificada nem culpada pelo resultado das catástrofes (HOWARD, 1994). O provável julgamento comprovadamente desinteressado de um sistema especialista poderia transformar-se num refúgio ainda melhor. Mesmo que um sistema de IA seja projetado com uma substituição do usuário, é uma obrigação considerar o incentivo na carreira de um burocrata que será pessoalmente responsabilizado se a substituição sair errada, e que preferiria muito mais culpar a IA por qualquer decisão difícil com um resultado negativo.[926]

Esse ponto nos leva a discutir de maneira mais aprofundada a responsabilidade moral desses agentes (ou actantes) não-humanos[927]. Para isso e

[925] DIAKOPOULOS, Nicholas. Algorithm Accountability – Journalistic investigation of computational power structures. *Digital Journalism*, v. 3, n. 3, p. 398, 2015: "Algorithmic accountability must therefore consider algorithms as objects of human creation and take into account intent, including that of any group or institutional processes that may have influenced their design, as well as the agency of human actors in interpreting the output of algorithms in the course of making higherlevel decisions."

[926] BOSTROM, Nick; YUDKOWSKY, Eliezer. A ética da inteligência artificial. *FUNDAMENTO – Revista de Pesquisa em Filosofia*, v. 1, n. 3, p. 202-203, 2011.

[927] Essa discussão complementa a análise sobre governança e toca as áreas de *Machine & Information Ethics e Philosophy of Technology*. Outra nomenclatura possível para essas questões é a de Ética Digital: "*Digital ethics is the branch of ethics that studies and evaluates moral problems related to data, algorithms and corresponding practices. Its goal is to formulate and support morally good solutions (e.g. right conducts or right values) by developing three lines of research: the ethics of data, the ethics of algorithms and the ethics of practices. The ethics of data looks at*

com o intuito de pensar em regulação, é crucial irmos além do mero reconhecimento do poder de agência das Coisas e buscarmos uma análise atenta às diferenças entre artefatos técnicos e sistemas sociotécnicos. Essa diferenciação se justifica em razão do nível de complexidade e potencial de influência de cada um, ensejando diferentes regulações, o que não se contradiz, mas, pelo contrário, complementa as perspectivas ator-rede e novo-materialista.

Na obra *Moralizing Technology: Understanding and Designing the Morality of Things*, Peter-Paul Verbeek pretende ampliar o alcance da ética para acomodar melhor a era tecnológica e, ao fazê-lo, revela a natureza inseparável da humanidade e da tecnologia. Para Verbeek, as tecnologias são "mediadores morais" que moldam a forma como percebemos e interagimos com o mundo e, desta forma, revelam e norteiam possíveis comportamentos. Nas palavras de Verbeek: "*No technology is morally neutral, since every technology always affects the way in which we perceive and interact with the world, and even the ways in which we think – it mediates our lives*."[928]

Com referência à teoria de Bruno Latour, citada neste trabalho, Verbeek conclui que a ética humanista necessariamente divide o mundo em dois domínios: o humano de um lado e o outro (ou o "não-humano") do outro, onde os seres humanos são sujeitos e os não-humanos são objetos de atividade humana. Como resultado dessa abordagem, torna-se quase impossível atribuir qualquer significância moral à tecnologia. Por essa razão partimos do cenário apresentado por Latour, segundo o qual, os artefatos também são atores sociais. Segundo o próprio Latour: [929]

> Conceber humanidade e tecnologia como pólos opostos é, com efeito, descartar a humanidade: somos animais sociotécnicos e toda interação humana é sociotécnica. Jamais estamos limitados a vínculos sociais. Jamais nos defrontamos unicamente com objetos. (...) A ilusão da modernidade foi acreditar que, quanto mais crescemos, mais se extremam a objetividade e a subjetividade,

---

the generation, recording, curation, processing, dissemination, sharing and use of data. It is concerned with moral problems posed by the collection, analysis and application of large data sets. Issues range from the use of big data in biomedical research and the social sciences to profiling, advertising and data donation and data philanthropy, as well as open data in government projects." Will Knight, "Forget Killer Robots...", MIT Technology Review, https://www.technologyreview.com/s/608986/forget-killer-robotsbias-is-the-real-ai-danger/

[928] VERBEEK, Peter-Paul. Moralizing Technology: Understanding and Designing the Morality of Things, Chicago / London, The University of Chicago Press, 2011.

[929] LATOUR, Bruno. A Esperança de Pandora: Ensaios sobre a realidade dos estudos científicos. Trad.: Gilson Cesar Cardoso de Sousa. São Paulo: EDUSC, 2001, p. 245.

> criando assim um futuro radicalmente diferente de nosso passado. Após a mudança de paradigma em nossa concepção de ciência e tecnologia, sabemos agora que isso nunca acontecerá e, na verdade, *nunca* aconteceu. (...) [Os artefatos] merecem ser alojados em nossa cultura intelectual como atores sociais de pleno direito. Os artefatos somos nós. O alvo de nossa filosofia, teoria social e moralidade cifra-se em inventar instituições políticas capazes de absorver essa grande história, esse vasto movimento em espiral, esse labirinto, esse fado.

Como se depreende desses ensinamentos de Latour, os artefatos são dotados de agência e possuem capacidade de interferir na realidade e, em razão disso, devem ser considerados atores sociais de pleno direito. Assim como os sistemas sociotécnicos, em uma escala ainda maior, o que se justifica pela sua maior complexidade, conforme veremos adiante.

Apesar da teoria de Latour enxergar o papel que cada actante possui colocando todos no mesmo patamar de agência, é importante considerarmos que não são todos os artefatos técnicos ou sistemas sociotécnicos que possuem a mesma capacidade de influência nas interações que ocorrem entre humanos e não-humanos. Por exemplo, a influência que uma porta física possui em relação a um indivíduo é consideravelmente distinta da influência gerada por uma Coisa dotada de inteligência artificial com algoritmos dotados de técnica de *deep learning*.[930]

Os artefatos técnicos, conforme nos explica o teórico holandês Peter Kroes, podem ser entendidos como *Coisas (objetos)* desenhados e feitos pelo homem, que possuem uma *função* e um *plano de uso*[931], bem como utensílios utilizados para sua fabricação. Consistem em produtos obtidos por meio da ação tecnológica, a qual designa as atitudes que tomamos no dia a dia com o intuito de resolver problemas práticos, incluindo aqueles ligados aos nossos desejos e às nossas necessidades[932]. Importante observar que os artefatos técnicos trazem consigo a necessidade de que regras de uso sejam observadas, bem como que sejam criados parâmetros em relação ao papéis dos indivíduos e das instituições sociais em relação a eles e a seu uso[933].

---

[930] *"Deep learning is a subset of machine learning in which the tasks are broken down and distributed onto machine learning algorithms that are organised in consecutive layers. Each layer builds up on the output from the previous layer. Together the layers constitute an artificial neural network that mimics the distributed approach to problem-solving carried out by neurons in a human brain." http://webfoundation.org/docs/2017/07/AI_Report_WF.pdf.*

[931] KROES, Peter. et al. *A Philosophy of Technology* From Technical Artefacts to Sociotechnical [s.l.]: Systems. Morgan & Claypool Publishers, 2011, pp. 1-2 e 5-7.

[932] Ibid, p. 1-2.

[933] Ibid, pp. 1-2 e 11.

Nas palavras de Kroes:[934]

> Problemas práticos não são resolvidos apenas introduzindo um conjunto de artefatos técnicos no mundo. Com estes artefatos vêm instruções para seu uso. E com artefatos técnicos, vêm também papéis sociais, para pessoas e instituições sociais que permitam o uso dos artefatos.[935]
> *(...)*
> Há uma grande variedade de artefatos técnicos - de muito pequenos a muito grandes, de simples a complexos, de componente a produto final e constituídos por materiais químicos, etc. O que todas essas coisas têm em comum é que eles são objetos materiais, produzidos deliberadamente pelos seres humanos para cumprir algum tipo de função prática. Muitas vezes são descritos como artefatos técnicos, a fim de enfatizar que não são objetos feitos naturalmente.[936]
> (…)
> Podemos, portanto, definir um artefato técnico como um objeto físico com uma função técnica e plano de uso projetado e feito por seres humanos. O requisito de que o objeto deve ser projetado e feito por humanos é adicionado para garantir que qualquer objeto natural que seja usado para fins práticos não seja também denominado "artefato técnico". Essas diferenças referem-se especialmente ao estado de ter uma função e um plano de uso, e à possibilidade de fazer afirmações normativas.[937]

Os artefatos técnicos, portanto, são objetos específicos (Coisas) com características próprias. Obras de arte, por exemplo, não são sinônimos de artefatos técnicos. Enquanto estes são criados pelo homem com claros objetivos práticos, aquelas não têm uma utilidade concreta e as habilidades exigidas para sua produção são diferentes das exigidas de engenheiros. Objetos naturais também não se confundem com os artefatos técnicos, visto que são dados pela natureza e não possuem, em si, uma função prática. Contudo, objetos naturais podem ser transformados em artefatos técnicos se passarem por um processo de transformação realizado pelo homem. Por exemplo: a madeira do tronco de uma

---

[934] Ibid, pp. 1-2 e 5-7.

[935] Tradução livre do autor. No original: *Practical problems are not just resolved by introducing a bunch of technical artefacts into the world. With these artefacts come instructions for their use. And with these technical artefacts come also social roles for people and social institutions for enabling the use of the artefacts.*

[936] Tradução livre do autor. No original: *There is a huge variety of technical artefacts from very small to very big, from simple to complex, from component part to end-product and consisting of chemical materials, et cetera. What all of these things have in common is that they are material objects that have been deliberately produced by humans in order to fulfil some kind of practical function. They are often described as technical artefacts in order to emphasise that they are not naturally occurring objects.*

[937] Tradução livre do autor. No original: *We may therefore define a technical artefact as a physical object with a technical function and use plan designed and made by human beings. The requirement that the object must be designed and made by humans is added to ensure that any natural objects that happen to be used for practical purposes are not also termed technical artefacts. Those differences relate especially to the status of having a function and a use plan, and to the accompanying possibility of making normative assertions.*

árvore é algo da natureza, mas passa a ser artefato técnico quando é transformada pelo homem num armário e ganha uma função concreta.

Por fim, os artefatos técnicos se diferenciam por dois pontos principais dos meros objetos físicos e de objetos biológicos. Em primeiro lugar, aqueles possuem função e plano de uso claros. Em segundo lugar, sujeitam-se à análise valorativa se são bons ou ruins e se funcionam ou não. [938] Assim, é possível observar a grande importância que a *função* e o *plano de uso* possuem na caracterização de um artefato técnico. Estas duas características estão intimamente conectadas com os objetivos que os indivíduos que criaram o objeto buscam com ele alcançar, de modo que elas não se separam das finalidades pretendidas.

Diante desta inseparabilidade, o questionamento sobre a moralidade dos objetivos e das ações humanas se estende à moralidade dos artefatos técnicos.[939] A tecnologia pode ser usada para mudar o mundo ao nosso redor e os indivíduos possuem objetivos – particulares e/ou sociais – que podem ser alcançados com o auxílio desses artefatos técnicos. Tendo em vista que os objetivos buscados pelo humano ao criar um artefato técnico não se separam das características do objeto produzido, podemos concluir que os artefatos técnicos possuem um caráter intrinsecamente moral.[940]

Este é um ponto importante ao qual deve ser dada a devida atenção, já que o debate sobre a responsabilidade por consequências geradas a partir da atuação dos objetos criados pelos humanos é ainda um ponto controverso: a responsabilidade caberá ao humano ou ao objeto? Voltaremos a essa discussão adiante, logo após conceituarmos sistemas sociotécnicos.

Portanto, ao lado dos artefatos técnicos, que podem representar desde os objetos mais simples e com pouca capacidade de interação/influência, até os tecnologicamente mais complexos, temos os sistemas sociotécnicos, que consistem em uma Rede (encaixando-se inclusive no conceito latouriano refletido

[938] KROES, Peter. et al. *A Philosophy of Technology* From Technical Artefacts to Sociotechnical [s.l.]: Systems. Morgan & Claypool Publishers, 2011, p. 7-13.
[939] Ibid, p. 9-10.
[940] Há um rico debate entre os estudiosos do tema sobre se determinados elementos como a consciência, o livre arbítrio, a espontaneidade, a criatividade e o papel da razão constituem ou não uma condição necessária para o reconhecimento de um agente moral (à semelhança do agente humano).

na teoria ator-rede) que conecta humanos e Coisas, possuindo, assim, maior capacidade de interação e também imprevisibilidade.

Para a análise regulatória, a atenção a esse conceito é ainda mais fundamental.[941] Justamente devido à sua complexidade consubstanciada em um conglomerado de actantes, fazendo com que os sistemas sociotécnicos possuam consequências ainda menos previsíveis do que aquelas geradas pelos artefatos técnicos. Além disso, geram uma maior dificuldade de se impedir consequências não premeditadas e também de responsabilização dos agentes em caso dano, uma vez que a "ação tecnológica" refletida no sistema sociotécnico é uma soma de ações de actantes entrelaçados na Rede em uma intra-relação[942].

Para ilustrar a diferença entre os conceitos de artefato técnico e sistema sociotécnico, podemos pensar no primeiro sendo representado por um avião e no segundo pelo complexo sistema de aviação. O sistema sociotécnico é formado pelo conjunto de agentes (actantes humanos e não-humanos (Coisas), instituições, etc) inter-relacionados que funcionam juntos para atingir determinado objetivo. A materialidade e efeitos de um sistema sociotécnico dependem do somatório da agência de cada actante. Porém, há parâmetros de como o sistema deve ser usado, o que significa que esses sistemas tem processos operacionais pré-definidos e podem ser afetados por leis e políticas regulamentadoras.

Dessa maneira, quando ocorre um trágico acidente envolvendo um avião, há que se analisar o que estava na esfera de controle e influência de cada ator e artefato técnico componentes desta Rede sociotécnica, mas muito possivelmente observaremos uma intra-ação relacional bastante complexa e simbiótica entre os componentes que levaram a esse fatídico resultado. [943] Além disso, esse resultado é muitas vezes imprevisível, em razão da autonomia do sistema baseada em uma agência difusa e distribuída entre todos os componentes (actantes). [944]

---

[941] KROES, Peter. et al. op.cit, pp. 1-2 e 67.

[942] Os conceitos de entrelaçamento (*entanglement*) e intra-ação encontram explicação aprofundada nos itens anteriores deste capítulo.

[943] SARAIVA, Leonardo. *Sistema de Análise de Erros Humanos na Prevenção De Acidentes Aeronáuticos*. 2011.

[944] Acadêmicos e empresas têm pesquisado as vulnerabilidades do setor de aviação, tentando propor uma solução que envolva aeronaves agrupadas, onde um grupo de aeronaves compartilham informações e validam as transmissões do outro, de modo que eles formam um grupo de "aeronaves de confiança", de forma que qualquer sinal falso seria rejeitado pelo grupo. Essas soluções estão tentando adicionar mais camadas de proteção em cima da tecnologia existente, minimizando riscos como hackeamento de aeronaves. Essas soluções se baseiam em uma

Segundo M. C. Elish, da Universidade de Columbia:[945]

> É comum ver um representante de companhia aérea no portão de um voo cancelado ouvindo gritos de viajantes frustrados, mesmo que ele não tenha causado o cancelamento, nem possua o poder de mudá-lo. Na linha de frente dos grandes sistemas burocráticos, as pessoas posicionadas como interface externa de um sistema aparecem, ao mesmo tempo, como uma metonímia para a empresa, e também como *gatekeepers*. Como gatekeepers, eles parecem possuir um grau de agência, uma capacidade de ação efetiva, que o cliente não possui. Mas em geral, sabemos que tais indivíduos não representam toda a empresa, e essa agência só é percebida, e não praticada. Sabemos, na maioria dos casos, esses indivíduos não são responsáveis pelas decisões que levaram à situação. Em casos como esses, os seres humanos na interface entre cliente e empresa são como esponjas, absorvendo o excesso de emoções que inundam a interação, mas não podem ser absorvidas por uma burocracia sem rosto ou objeto inanimado. Pode haver ramificações afetivas por uma culpa errônea, mas o cliente ou gerente que tiver conhecimento, saberá que o indivíduo não é responsável. No entanto, em sistemas automatizados ou robotizados, pode ser difícil localizar com precisão quem é responsável quando a agência é distribuída em um sistema e o controle sobre uma ação é mediada pelo tempo e espaço. Quando humanos e máquinas trabalham juntas, quem ou o que está no controle? Como o controle se distribuiu em vários atores (humanos e não humanos), nossas concepções sociais e jurídicas de responsabilidade permaneceram em relação ao indivíduo, de forma geral. Desenvolvemos o termo "zona de deformação moral" para descrever o resultado dessa ambigüidade dentro de sistemas de controle distribuído, particularmente sistemas automatizados e autônomos. Assim como a "zona de deformação" em um carro é projetada para absorver a força do impacto em um acidente, o humano em um sistema altamente complexo e automatizado pode tornar-se simplesmente um componente - acidental ou intencionalmente - que tem o peso das responsabilidades morais e legais quando há mau funcionamento geral do sistema.[946]

---

perspectiva que enxerga não somente os aviões como artefatos técnicos isolados, mas pensando em soluções que envolvam o sistema sociotécnico de forma mais ampla. http://www.airport-technology.com/features/featureair-traffic-control-easy-target-hackers/.

[945] ELISH, M. MORAL CRUMPLE ZONES: CAUTIONARY TALES IN HUMAN-ROBOT INTERACTION. 2016.

[946] Tradução livre do autor. No original: *It is common to see an airline representative at the gate of a canceled flight be yelled at by frustrated travelers, even though he neither caused the cancelation nor possesses the power to change it. On the front lines of large, bureaucratic systems, people positioned as the external interface of a system appear at once a metonym for the company and also as gatekeepers to the company. As gatekeepers, they seem to possess a degree of agency, a capacity to take effective action, which the customer does not. But in general, we know that such individuals do not represent the whole company, and that agency is only perceived, not actuated. We know, in most cases, these individuals are not responsible for the decisions that have led up to the situation. In instances like these, humans at the interface between customer and company are like sponges, soaking up the excess of emotions that flood the interaction but cannot be absorbed by faceless bureaucracy or an inanimate object. There may be affective ramifications for this misplaced blame, but the discerning customer or manager will know that the individual is not responsible. However, in automated or robotic systems it can be difficult to accurately locate who is responsible when agency is distributed in a system and control over an action is mediated through time and space. When humans and machines work together, who or what is in control? As control has become distributed across multiple actors (human and nonhuman), our social and legal conceptions of responsibility have remained generally about an individual. We developed the term moral crumple zone to describe the result of this ambiguity within systems of distributed*

Com esses sistemas complexos, o debate sobre a responsabilidade e eticidade – já levantado quando da apresentação dos artefatos técnicos – retorna. Questões como a responsabilização dos desenvolvedores e sobre a existência de moralidade em actantes não-humanos – com foco, aqui, em objetos tecnológicos – precisa de uma resposta ou, ao menos, de reflexões que contribuam para o debate na esfera pública. [947]

A teoria de Latour oferece grande avanço ao enfrentar e descartar a divisão binária formal entre humanos e não-humanos, mas ela coloca objetos com complexidades e importâncias distintas no mesmo nível. Diante desse contexto, do ponto de vista jurídico e regulatório, justifica-se atribuirmos diferentes status a artefatos técnicos e sistemas sociotécnicos de acordo com sua capacidade de agência e de influência, devendo ser dotados de diferentes status moral e nível de responsabilidade. É preciso então distinguir a influência e a importância que cada Coisa possui na Rede e, sobretudo, na esfera pública para, a partir daí, pensar o que pode ser feito, sob o ponto de vista ético-regulatório, no cenário de IoT.

Para essa análise, focaremos a partir de agora em algoritmos avançados com *machine learning* e em robôs dotados de inteligência artificial tendo em vista que constituem artefatos técnicos (Coisas) agregados a sistemas sociotécnicos com um potencial maior de autonomia (baseada em grande medida no processamento de *Big Data*) e imprevisibilidade.

Enquanto artefatos técnicos como uma cadeira ou um copo constituem artefatos já "domesticados" pelo homem, ou seja, mais previsíveis em relação aos riscos de sua influência e poder de agência, podemos dizer que algoritmos e robôs inteligentes ainda são tecnologias não-domesticadas, uma vez que o tempo de interação com o homem ao longo de sua história não permitiu ainda prever a maioria dos riscos de forma a controlá-los ou cessá-los por completo. Esse recorte nos permitirá trabalhar o tema de ética das Coisas em sua vertente mais complexa.

---

control, particularly automated and autonomous systems. Just as the crumple zone in a car is designed to absorb the force of impact in a crash, the human in a highly complex and automated system may become simply a component— accidentally or intentionally—that bears the brunt of the moral and legal responsibilities when the overall system malfunctions.

[947] Em sua definição habermasiana.

Colin Allen e Wendell Wallach[948] argumentam que, à medida que Coisas inteligentes como os robôs[949] possuem cada vez mais autonomia e assumem cada vez mais responsabilidade, eles devem ser programados com habilidades morais de decisão, para nossa própria segurança.[950]

Corroborando com essa tese, Peter-Paul Verbeek [951] ao tratar da moralidade das Coisas entende que: como as máquinas[952] operam com mais freqüência do que antes em ambientes sociais abertos como esferas públicas conectadas, torna-se cada vez mais importante projetar um tipo de moral funcional que seja sensível às características eticamente relevantes e aplicáveis às situações que se pretende. Com relação a qual tipo de ética implementar, defende-se neste trabalho que seja de matriz deontológica e construída dentro dos parâmetros procedimentais deliberativos defendidos por Habermas, mas enxergando o poder de agência das Coisas em uma perspectiva novo-materialista.

O exemplo utilizado no subtópico III.II deste trabalho para endereçar o debate da esfera pública de Habermas – caso do robô Tay, da Microsoft -, novamente ajudará a ilustrar os efeitos que um elemento não-humano pode gerar na sociedade. Como ora elucidado, a Microsoft lançou em 2016 um programa de Inteligência Artificial que denominou Tay. Dotado de capacidade de *deep learning*[953], o robô moldava sua visão de mundo baseando-se na interação online com outras pessoas e produzindo expressões autênticas a partir delas. A experiência, contudo, se mostrou desastrosa e a companhia teve de desativar a

[948] WALLACH, Wendell; ALLEN Colin,. *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press, 2008.

[949] O Relatório de Robótica do Mundo da ONU 2005 define um robô como uma máquina reprogramável semi ou totalmente autônoma empregada para o bem-estar dos seres humanos nas operações de fabricação ou serviços.

[950] Em complemento, os pesquisadores da Delft University of Technology e da Eindhoven University of Technology[950]sustentam que os valores que devem ser levados em consideração no desenvolvimento destas tecnologias são: saúde, segurança, sustentabilidade e privacidade.

[951] VERBEEK, Peter-Paul. *Moralizing Technology:* Understanding and Designing the Morality of Things, Chicago / London, The University of Chicago Press, 2011.

[952] *"Artificial intelligence theorists distill the concept of full autonomy down to the paradigm of machines that "sense-think-act" without human involvement or intervention. And Oxford Professor Nick Bostrom, an eminent futurist, goes as far as to suggest that machines capable of independent initiative and of making their own plans . . . are perhaps more appropriately viewed as persons than machines." https://perma.cc/EJ5M-YMCJ.*

[953] Conceito já explicado anteriomente neste trabalho.

ferramenta em menos de 24 horas depois do início de seu funcionamento, em função da produção de resultados preocupantes.[954]

O objetivo era fazer com que Tay interagisse com usuários humanos no Twitter, por meio da Internet, e que, a partir daí, aprendesse padrões humanos de conversa. Ocorre que, em menos de um dia, o *chatbot* estava gerando comentários absolutamente inapropriados, incluindo publicações racistas, sexistas e anti-semitas. O caso possui semelhanças com o que ocorreu em 2015 com o "Google Photos". Esse era um programa que também aprendia com os usuários, mas desta vez, para dar *labels* a fotos. Contudo, os seus resultados também foram desagradáveis e se percebeu, por exemplo, que o *bot* estava dando o *label* de gorilla a fotos de pessoas negras.[955]

Claramente, a aplicação de programas capazes de "aprender" para desempenhar algum tipo de função com as pessoas gera novos desafios éticos e regulatórios, uma vez que se aumenta a possibilidade de se obterem resultados diversos dos pretendidos ou mesmo totalmente inesperados. Além disso, esses resultados podem gerar danos a outros atores, como as ofensas discriminatórias geradas pelo Tay e pelo Google Photos.

Especialmente, o emprego de ferramentas de inteligência artificial que interagem por meio de mídias sociais exige que se reflita sobre os requisitos éticos que devem acompanhar o desenvolvimento desse tipo de tecnologia. Isso porque, como defendido anteriormente, esses mecanismos também atuam como agentes em sociedade, e acabam influenciando o meio à sua volta, mesmo sendo elementos não-humanos. Não se trata, portanto, de pensar apenas sobre o "uso" e o "conserto" das novas tecnologias, mas principalmente sobre o norteamento ético adequado para seu desenvolvimento.[956]

A Microsoft afirmou que o mau-funcionamento de Tay foi resultado de um ataque realizado por usuários que exploraram uma vulnerabilidade no seu programa. Contudo, para Wolf et al.[957], isso não os exime da responsabilidade de

[954] Disponível em: <https://tecnoblog.net/193318/tay-robo-racista-microsoft/>. Acesso em 27 set. 2017.
[955] Disponível em: <https://www.tecmundo.com.br/google-fotos/82458-polemica-sistema-google-fotos-identifica-pessoas-negras-gorilas.htm>. Acesso em 27 set. 2017.
[956] WOLF, Marty, et al. *Why We Should Have Seen That Coming:* Comments on Microsoft's tay "Experiment," and Wider Implications. 2017. Disponível em: <http://digitalcommons.sacredheart.edu/computersci_fac/102/>. Acesso em 27 set. 2017.
[957] Ibid.

considerar a ocorrência de possíveis consequências danosas com o emprego desse tipo de software. Isso porque, para os autores, o fato de os seus criadores não terem esperado que acontecesse o que se verificou com a Tay faz parte da própria natureza imprevisível desse tipo de sistema.

A tentativa de se fazer com que sistemas de Inteligência Artificial se tornem cada vez mais adaptáveis e capazes de agir de forma semelhante a humanos os faz apresentar comportamentos menos previsíveis. Assim, passam a atuar não somente como ferramentas que exercem funções pré-estabelecidas nos diversos campos em que são empregados, mas também a desenvolver uma forma própria de agir. Desse modo, produzem impactos no mundo de forma cada vez menos determinável ou controlável por agentes humanos. Vale destacar que algoritmos podem se ajustar para originar novos algoritmos e novas formas de realizar suas tarefas[958], de modo que a forma pela qual se chegou ao resultado seria algo difícil de explicar até mesmo para os programadores que criaram o algoritmo[959].

Além disso, quanto mais adaptáveis se tornam os programas de inteligência artificial, mais imprevisíveis passam a ser suas ações, trazendo novos riscos. Isso faz com que seja necessário que os desenvolvedores desse tipo de programa estejam mais atentos às responsabilidades éticas envolvidas nessa atividade. O Código de Ética da *Association for Computing Machinery*[960] indica que os profissionais da área devem desenvolver "avaliações abrangentes e completas dos sistemas informáticos e seus impactos, inclusive a análise de possíveis riscos".

Além disso, é necessário que haja um monitoramento dedicado a verificar as ações desempenhadas por um programa deste tipo, especialmente nos estágios iniciais de sua implementação. No caso Tay, os desenvolvedores deveriam ter

[958] Sobre os *learning algorithms*, confira-se a explicação de Pedro Domingos: "Every algorithm has an input and an output: the data goes into the computer, the algorithm does what it will with it, and out comes the result. Machine learning turns this around: in goes the data and the desired result and out comes the algorithm that turns one into the other. Learning algorithms—also known as learners—are algorithms that make other algorithms. With machine learning, computers write their own programs, so we don't have to." (DOMINGOS, Pedro. The Master Algorithm: how the quest for the ultimate learning machine will remake our world. New York: Basic Books, 2015).

[959] DONEDA, Danilo; ALMEIDA, Virgilio A. F. What Is Algorithm Governance? *IEEE Internet Computing*, v. 20, p. 60, 2016.

[960] WOLF, Marty, et al. *Why We Should Have Seen That Coming:* Comments on Microsoft's tay "Experiment," and Wider Implications. 2017. Disponível em: <http://digitalcommons.sacredheart.edu/computersci_fac/102/>. Acesso em 27 set. 2017.

monitorado o comportamento do *bot* de forma intensa nas primeiras 24 horas de seu lançamento, o que não se sabe se ocorreu.[961]

Ademais, não há como determinar com certeza o que motivou a Microsoft a retirar o programa do ar: se a produção de comentários ofensivos ou a resposta negativa recebida por parte dos usuários em relação ao programa. A ideia deve passar mais por uma lógica de prevenção de possíveis danos e de monitoramento do que remediação desses prejuízos, em especial quando podem ser imprevisíveis. Para que se limitem as possibilidades de consequências negativas, os desenvolvedores de software devem reconhecer aqueles programas potencialmente perigosos e imprevisíveis, e restringir as suas possibilidades de interação com o público até que seja intensamente testado em um ambiente controlado. Depois dessa fase, os consumidores devem ser informados sobre as vulnerabilidades de um programa que é, em essência, imprevisível, e das possíveis consequências de um comportamento inesperado.[962]

Outro caso[963] envolvendo inteligência artificial ocorreu em novembro de 2016, quando o Google Tradutor desenvolveu uma linguagem própria ininteligível para humanos. Alguns meses antes, o Google havia instalado o sistema *Google Neural Machine Translation*, que aprenderia a traduzir com base em exemplos e atingir precisão cirúrgica na sua tarefa. O mecanismo teria sido programado para traduzir determinadas línguas e deveria passar pelo inglês. O sistema conseguiu, porém, traduzir línguas diretamente sem a interferência do inglês, o que significa dizer que o sistema de inteligência artificial teria desenvolvido uma língua própria, uma *interlíngua*[964].

---

[961] Ibid.

[962] WOLF, Marty, et al. Why We Should Have Seen That Coming: Comments on Microsoft's tay "Experiment," and Wider Implications. 2017. Disponível em: <http://digitalcommons.sacredheart.edu/computersci_fac/102/>. Acesso em 27 set. 2017.

[963] Outro caso interessante que nos ajuda a pensar na autonomia desses agentes é a criação e a adoção do Tinder. Estima-se um número total de 50 milhões de usuários. Essa plataforma intermedia encontros entre diferentes pessoas que buscam se relacionar umas com as outras. Hoje, portanto, mesmo relações consideradas de maior intimidade são engendradas e possibilitadas pelo uso de aplicativos como este. De fato, o algoritmo que sustenta o programa é responsável por "decidir" quem aparecerá para quem, a partir de critérios desconhecidos pelos usuários. Assim, as interações entre as pessoas registradas são estabelecidas e influenciadas pelo emprego do código do programa e da filtragem algorítmica, de modo que esse elemento - não-humano – exerce influência sobre essas relações.

[964] SUMARES, Gustavo. Sistema do Google inventou uma língua própria que humanos não entendem. *Olhar Digital*, nov. 2016. Disponível em: <https://olhardigital.com.br/pro/noticia/sistema-do-google-inventou-uma-lingua-propria-que-humanos-nao-entendem/64122>. Acesso em: 16 ago. 2017.

Situação similar ocorreu recentemente com a inteligência artificial desenvolvida pelo Facebook. O sistema teria sido criado para que Bob e Alice – nomes dados aos *bots* criados pelos pesquisadores – simulassem negociações em inglês afim de ajudar os pesquisadores a entender formas mais construtivas de negociação. Contudo, Bob e Alice se entendiam melhor usando frases ininteligíveis para humanos e, assim, chegavam a acordos mais rapidamente. O sistema foi desativado e não gerou resultados positivos para a pesquisa[965].

Como se depreende desses exemplos – que, destaque-se, tendem a se multiplicar –, o uso da tecnologia, com enfoque na inteligência artificial, pode gerar consequências imprevisíveis e incontroláveis, de modo que, muitas vezes, a única solução é desativar o sistema. Fica claro, portanto, o ganho de autonomia e complexidade dos novos artefatos técnicos, visto que são dotados de agência incrementada, capaz de influenciar e serem influenciadas na rede de maneira significativa, compondo muitas vezes sistemas sociotécnicos ainda mais autônomos e imprevisíveis.

Embora não exista um sistema de inteligência artificial que seja completamente autônomo, imagina-se que, com o desenvolvimento da tecnologia, é possível que sejam criadas máquinas que terão a capacidade de tomar decisões de forma cada vez mais autônoma, o que levanta questões acerca de quem seria o responsável pelo resultado de suas ações e por eventuais reparações pelos danos gerados.[966].[967] Segundo Relatório divulgado no Fórum Econômico Mundial de 2017:[968] *The greatest threat to humanity lies in delegating authority and decisions to machines that they do not have the intelligence to make.*

A habilidade de acumular experiências e aprender com base em processamentos massivos de dados, somada à capacidade de agir de forma independente e fazer escolhas de maneira autônoma podem ser consideradas pré-condições para a responsabilidade por danos. Contudo, como não se reconhece

[965] SUMARES, Gustavo. Facebook desativa inteligência artificial que criou linguagem própria. *Olhar Digital*, jul. 2017. Disponível em: <https://olhardigital.com.br/noticia/facebook-desativa-inteligencia-artificial-apos-ela-criar-sua-propria-linguagem/70075>. Acesso em: 16 ago. 2017.
[966] VLADECK, David C. Machines without principals: liability rules and artificial intelligence. *Washington Law Review*, vol. 89, n. 1, mar. 2014. p. 120-121.
[967] CERKA, Paulius et al. Liability for damages caused by artificial intelligence. *Computer Law & Security Review*, vol. 31, n. 3, jun. 2015. p. 376 – 389.
[968] Disponível em: <https://weforum.ent.box.com/v/AI4Good?platform=hootsuite>. Acesso em 27 set. 2017.

hoje a Inteligência Artificial como um sujeito de direito, ela não pode ser considerada individualmente responsável pelos potenciais danos que pode causar.[969] Nesse sentido, segundo o art. 12 da Convenção das Nações Unidas sobre o Uso de Comunicações Eletrônicas em Contratos Internacionais, uma pessoa (natural ou uma entidade) em nome de quem um programa foi criado deve, em última análise, deve ser responsável por qualquer ação gerada pela máquina. Esse raciocínio pauta-se pela noção de que uma ferramenta não possui vontade própria.[970]

Por outro ângulo, no caso de danos causados por atos de uma inteligência artificial, outro tipo de responsabilidade aventada é aquela que faz uma analogia com a responsabilidade atribuída aos pais pelas ações de seus filhos (*strict vicarious liability)*. Dessa forma, adotando-se a teoria de "robôs como ferramentas", a responsabilidade pelos atos de uma AI poderia recair sobre seu produtor, usuários ou seus programadores, responsáveis pelo seu "treinamento"[971] .[972]

Outra possibilidade é o modelo que foca na habilidade de os programadores ou usuários preverem o potencial de ocorrência desses delitos.

[969] CERKA, Paulius et al. op.cit.
[970] Ibid.
[971] O problema desta abordagem é que as Coisas começam a partir de agora a se treinar sem que seja necessário um input humano. A evolução desssa característica costuma ter a seguinte narrativa: "Há pouco mais de 20 anos, em 1997, o campeão de xadrez, Garry Kasparov, perdeu seu reinado para o supercomputador Deep Blue. Se em 1997 o Deep Blue fez história, em 2017 foi a vez de outro supercomputador, o Alpha Go Zero, que venceu diversos adversários humanos no complexo jogo "Go". De fato, desde 2015, sua versão anterior, o Alpha Go, já vinha dominando as manchetes ao vencer, sucessivamente, os melhores jogadores de Go, em grande medida pela capacidade de reunir dados de seus oponentes e aprender com as partidas até então disputadas. Os resultados obtidos pelo Alpha Go Zero são relevantes porque advém de uma técnica de inteligência artificial chamada "*reinforcement learning*" ou "aprendizado via reforço", somente possível graças à capacidade de armazenar, processar e analisar dados, hábitos e táticas dos jogadores. Trata-se de uma técnica na qual, ao experimentar diferentes abordagens para um problema, o computador aprende qual a melhor solução, sem, no entanto, necessitar de qualquer programação ou ensinamento prévio por parte de um humano. Dessa forma, o computador torna-se capaz de fazer coisas sem que nenhum programador tenha que ensiná-lo previamente. O Alpha Go Zero foi treinado apenas a partir de sua própria experiência com a gestão de dados pessoais dos jogadores e partidas, o que o permite superar as capacidades humanas e operar em domínios em que falta conhecimento aos humanos. No mesmo sentido, a mais nova versão do supercomputador AlphaZero, também por meio da técnica de *reinforcement learning,* dominou o jogo em apenas quatro horas depois de ser programado com as regras do xadrez (sem quaisquer estratégias), tendo sido capaz de derrotar o melhor programa de computador de xadrez até então, o Stockfish." https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/inteligencia-artificial-protecao-de-dados-e-o-futuro-das-invencoes-26012018
[972] CERKA, Paulius et al. Liability for damages caused by artificial intelligence. *Computer Law & Security Review*, vol. 31, n. 3, jun. 2015. p. 376 – 389.

Segundo este segundo modelo, uma pessoa pode ser considerada responsável por um delito se ele representa uma consequência natural e provável da conduta daquela pessoa. Ele requer apenas que o programador ou usuário tenha agido com dolo ou tenha sido negligente[973] em face de um resultado que seria previsível.[974]

Em complemento, a respeito da responsabilidade civil, George S. Cole trata de quatro tipos: (i) a responsabilidade por produto, (ii) a responsabilidade por serviço, (iii) imperícia (*malpractice*)*, e* (iv) negligência.[975] O autor afirma que a disciplina da responsabilidade de produto é, no melhor dos casos, apenas parcialmente aplicável. Os elementos básicos para a sua aplicabilidade seriam: (i) a AI deve ser um "produto"; (ii) o réu deve ser um vendedor da AI; (iii) A AI deve alcançar a parte prejudicada sem alteração substantiva; (iv) a AI deve ser defeituosa; e (v) o defeito deve ser a origem do dano. Já a responsabilidade por serviço seria, na visão do autor, melhor aplicada, mas pouco definida.[976] Por outro lado, o autor sustenta que a aplicação da disciplina da responsabilidade por imperícia, por sua vez, possui grande potencial.[977] Se encontraria, dessa forma, entre a responsabilidade objetiva (*strict liability*) e a negligência. O standard, nesse caso, deveria ser fixado pela comunidade profissional.[978]

No entanto, enquanto o campo se desenvolve, para Cole, modelo da negligência seria o mais aplicável. Porém, ele pode ser difícil de ser implementado, principalmente quando alguns erros são totalmente imprevisíveis ou até mesmo inevitáveis. Até hoje, os tribunais ainda não formularam uma definição clara do dever envolvido na criação de AIs que, caso não observado, deveria ensejar uma responsabilidade por negligência.[979]

Caso um ato de uma Inteligência Artificial cause danos em razão de dolo ou negligência, de defeito de fabricação ou falha de design como resultado de uma programação deficiente, as regras existentes de responsabilidade indicariam na

---

[973] Andrews, 75 F.3d at 552.
[974] HALLEVY, Gabriel. The Criminal Liability of Artificial Intelligence Entities: From Science Fiction to Legal Social Control. *Akron Intellectual Property Journal*, vol. 4, 2010.
[975] COLE, George S. Tort Liability For Artificial Intelligence And Expert Systems. *Computer/Law Journal*, vol. 10, n. 2, 1990.
[976] Ibid.
[977] Em razão de o texto ter sido produzido em 1990, o autor afirma que o modelo da responsabilidade por imperícia ainda não seria aplicável, porque a programação não constituía oficialmente uma profissão. Contudo, esse conceito deve ser atualizado, já que hoje essa profissão é amplamente reconhecida.
[978] COLE, George S. 1990, op.cit.
[979] Ibid.

maioria das vezes a "culpa" dos seus criadores. No entanto, muitas vezes não é fácil saber como esses programas chegam às suas conclusões ou mesmo passam a gerar consequências inesperadas e possivelmente desagradáveis. Esse potencial nocivo é especialmente perigoso no emprego de programas de Inteligência Artificial que contam com mecanismos de aprendizagem de máquinas (*machine learning*), em que a própria natureza do *software* envolve a intenção de desenvolver uma atuação que não é previsível, e que apenas será determinada a partir dos dados e eventos com os quais o programa entra em contato.

Cientistas de diversas áreas se preocupam e ponderam que conferir essa capacidade de "pensamento" autônomo às máquinas necessariamente pode lhes conferir a capacidade de agir de forma contrária às regras que lhes são dadas[980].[981] Por isso a importância de se levar em consideração e investigar as esferas de controle e influência dos designers e outros agentes durante a criação e o desenvolvimento funcional dos artefatos técnicos.[982][983]

Muitas vezes, durante a fase de design, as consequências são indeterminadas pois dependem parcialmente das ações de outros fatores e agentes além dos designers. Além disso, como a tomada de uma decisão pode ser um processo complexo, é possível que seja difícil para um humano até mesmo explicá-la. Pode ser difícil, ainda, provar que o produto que contém a AI era defeituoso, e, especialmente, que o defeito já existia quando de sua produção.[984]

Pelo fato do comportamento de uma AI não ser totalmente previsível e seu comportamento ser o resultado da interação entre diversos agentes humanos e

[980] PAGALLO, Ugo. *The Law of Robots*: Crimes, Contracts and Torts. Berlim: Springer Science & Business Media 2013.
[981] VLADECK, David C. Machines without principals: liability rules and artificial intelligence. *Washington Law Review*, vol. 89, n. 1, mar. 2014. p. 120-121.
[982] Nessa linha, surgem alguns questionamentos relevantes: Seria possível apontar como responsáveis as companhias que projetaram, programaram, ou manufaturaram a máquina, mesmo que tenham inserido nessa programação regras que impediriam um comportamento prejudicial a humanos? Deveriam os criadores ser responsabilizados de forma total em qualquer ocasião em que algo dê errado, mesmo quando as máquinas projetadas se "auto-ensinam"? Nesse caso, a conduta geradora de dano já seria uma prova de defeito? Ou se adotaria uma teoria que valoriza a posição econômica do sujeito para a responsabilização, de que os criadores estão em uma posição melhor para absorver o custo do dano do que a pessoa prejudicada?
[983] É responsabilidade dos engenheiros pensar nos valores que entrarão no design dos artefatos, na sua função e no seu manual de uso. O que escapa do design e do manual de uso não depende do controle e influência do engenheiro e pode ser imprevisível. Por isso engenheiros devem projetar artefatos técnicos sensíveis a valores. Um artefato sensível a valores constitucionalmente garantidos (deliberados na esfera pública) é um artefato responsável.
[984] CERKA, Paulius et al. Liability for damages caused by artificial intelligence. *Computer Law & Security Review*, vol. 31, n. 3, jun. 2015. p. 376 – 389.

não-humanos que compõem o sistema sociotécnico e até mesmo de processos de *self-learning*, pode ser extremamente difícil encontrar o nexo causal[985] entre o dano gerado e a ação de um ser humano ou pessoa jurídica.[986]

Pelo arcabouço jurídico que temos hoje, isso pode levar a uma situação de "irresponsabilidade distribuída" (denominação atribuída no presente trabalho para se referir ao possível efeito decorrente da falta de identificação do nexo causal entre a conduta do agente e o dano produzido) entre os diferentes actantes envolvidos no processo. Isso ocorrerá principalmente quando o dano ocorrer dentro de um complexo sistema sociotécnico, no qual não será óbvia a responsabilidade da Coisa inteligente em si, nem de uma pessoa física ou jurídica.[987]

[985] Entende-se por 'nexo causal' o vínculo existente entre a conduta do agente e o resultado por ela produzido. "Examinar o nexo de causalidade é descobrir quais condutas, positivas ou negativas, deram causa ao resultado previsto em lei. Assim, para se dizer que alguém causou um determinado fato, faz-se necessário estabelecer a ligação entre a sua conduta e o resultado gerado, isto é, verificar se de sua ação ou omissão adveio o resultado." Disponível em: < https://www.jusbrasil.com.br/topicos/291656/nexo-causal>. Acesso em 27 set. 2017.

[986] Caitlin Sampaio Mulholland abordou a problemática da irresponsabilidade distribuída (denominação atribuída no presente trabalho para se referir ao efeito decorrente da falta de identificação do nexo causal entre a conduta do agente e o dano produzido) em sua tese sobre presunção de causalidade. Em arejada análise, Caitlin Mulholland enfrenta o cenário de falta de clareza no nexo causal entre os agentes reforçando o conceito de "causalidade alternativa". O conceito de casualidade alternativa permite identificar que o dano foi causado por uma única conduta que, devido à característica de coesão do grupo, resta impossível de atestar. O objetivo desta responsabilidade é buscar o ressarcimento da vítima, presumindo-se o nexo de causalidade. Segundo Mulholland: "No caso de existirem várias atividades, sendo que cada uma delas, por si só, teria sido suficiente para produzir o dano, mas em que persiste incerteza sobre qual efetivamente o causou, cada uma será considerada como causa do dano até o limite correspondente à probabilidade de o ter causado". (...) Existe um único nexo causal que não pode ser identificado de forma direta. Daí a sua presunção em relação ao grupo como um todo. (...) O que se busca com a causalidade alternativa é possibilitar a reparação dos danos causados através da facilitação do ônus probatório. Ao invés de a vítima ter que provar que determinada pessoa através de sua conduta causou o dano que a afligiu, poderá contar com a presunção da causalidade, sendo suficiente que prove que sofreu um dano e que o dano foi conseqüência de determinada atividade realizada por um determinado grupo." A tese defendida por Mulholland vai além, portanto, dos casos de: (a) responsabilidade solidária entre os imputados causadores do dano; (b) responsabilidade atribuída de acordo com a contribuição causal de cada agente para a obtenção do resultado danoso; (c) a responsabilidade atribuída somente a um dos agentes, quando for possível identificar o rompimento do nexo de causalidade entre as condutas sucessivas. Quando pensamos, no entanto, nos danos causados dentro de sistemas sociotécnicos, temos uma aplicação de nexo causal e de responsabilidade ainda mais complexo. Isso porque estamos falando muitas vezes da ação causada por um somatório de agências de seres humanos, instituições e coisas inteligentes com autonomia e poder de agência próprio. Nesse caso, o foco no grupo econômico, apesar de conseguir responder a diversos casos de dano, pode não ser suficiente para a atribuição justa de responsabilidade na era de IoT e de inteligência artificial forte. MULHOLLAND, Caitlin Sampaio. A responsabilidade civil por presunção de causalidade. Rio de Janeiro: GZ, 2010.

[987] Disponível em: <http://unesdoc.unesco.org/images/0025/002539/253952E.pdf>. Acesso em 27 set. 2017.

Segundo sustentam os pesquisadores do Alan Turing e Oxford Internet Institute:[988]

> O design modular dos sistemas pode significar que nenhuma pessoa ou grupo pode entender completamente a maneira pela qual o sistema irá interagir ou responder a um fluxo complexo de novas entradas. "Da programação linear tradicional aos algoritmos autônomos, o controle comportamental é gradualmente transferido do programador para o algoritmo e seu ambiente operacional. A diferença entre o controle do designer e o comportamento do algoritmo cria uma lacuna de responsabilização em que a culpa pode potencialmente ser atribuída a vários agentes morais simultaneamente.[989]

Corroborando com essa tese, segundo o recente Report[990] da UNESCO sobre "*robotics ethics*":

> O desenvolvimento rápido de robôs autônomos altamente inteligentes, provavelmente desafiará nossa classificação atual de seres de acordo com seu status moral, da mesma forma, ou talvez, mais profundamente, que aconteceu com animais não humanos através do movimento pelos direitos dos animais. Pode até mesmo alterar a forma como o *status* moral humano é atualmente percebido. Embora ainda pareça especulação futurista, questões como essas não devem ser descartadas, especialmente tendo em vista que a "divisão homem-máquina" está desaparecendo gradualmente e a probabilidade de aparência futura de híbridos humano-máquina ou animal-máquina ou cyborgs (robôs integrados com organismos biológicos ou pelo menos contendo alguns componentes biológicos). (...) Em todos esses casos, parece haver uma responsabilidade "compartilhada" ou "distribuída" entre designers de robôs, engenheiros, programadores, fabricantes, investidores, vendedores e usuários. Nenhum desses agentes pode ser indicado como a última fonte de ação. Ao mesmo tempo, esta solução tende a diluir completamente a noção de responsabilidade: se todos tiverem uma parte na responsabilidade total, ninguém será completamente responsável. Este problema é conhecido como o "problema de muitas mãos". (...) Os robôs podem ser usados para fins destinados por seus designers, mas também para outros fins, especialmente se o seu "comportamento" puder ser "pirateado" ou "reprogramado" por seus usuários finais. Os robôs podem apresentar implicações muito além das intenções de seus desenvolvedores. É impossível para os roboticistas preverem inteiramente como seu trabalho poderá afetar a sociedade.[991]

---

[988] Mittelstadt, Brent, et al. The ethics of algorithms: Mapping the debate. *Big Data & Society* July–December 2016.

[989] Tradução livre do autor. No original: *The modular design of systems can mean that no single person or group can fully grasp the manner in which the system will interact or respond to a complex flow of new inputs.'' From traditional, linear programming through to autonomous algorithms, behavioural control is gradually transferred from the programmer to the algorithm and its operating environment. The gap between the designer's control and algorithm's behaviour creates an accountability gap wherein blame can potentially be assigned to several moral agents simultaneously.*

[990] Disponível em: <http://unesdoc.unesco.org/images/0025/002539/253952E.pdf>. Acesso em 27 set. 2017.

[991] Tradução livre do autor. No original: *The rapid development of highly intelligent autonomous robots, then, is likely to challenge our current classification of beings according to their moral*

Outro ponto interessante a se considerar nesse contexto, é que falhas são naturais e podem ser consideradas até desejáveis para o aprimoramento mais célere de um artefato técnico. Portanto, não cabe pensarmos em um cenário regulatório para extinguir a possibilidade de falhas ou de danos e sim para melhor guiar seu desenvolvimento e gerenciá-lo sob uma ótica de proteção de direitos fundamentais.

Ainda não se encontraram respostas seguras para a questão de como lidar com os danos potenciais que poderão surgir em razão de erros de programação, ou mesmo em função de processos de *machine learning* que acabam por incorporar ao comportamento da máquina condutas indesejadas que não foram previstas pelos desenvolvedores [992] . Portanto, tão importante quanto trabalhar no desenvolvimento dessas novas tecnologias é discutir e estabelecer fundamentos éticos mínimos para regular o que se busca produzir.

No caso da Inteligência Artificial, é essencial que se trave um amplo debate acerca das diretrizes éticas que deverão guiar a construção dessas máquinas. Afinal, vê-se um crescimento muito forte desse segmento da pesquisa científica [993] , inclusive no cenário regulatório, sem que se tenha definido

---

status, in the same or maybe even more profound way as it happened with non-human animals through the animal rights movement. It may even alter the way in which human moral status is currently perceived. Although still resembling futuristic speculations, questions like these should not be dismissed lightly, especially in view of the fact that the 'human-machine divide' is gradually disappearing and the likelihood of future appearance of human-machine or animal-machine hybrids or cyborgs (robots integrated with biological organisms or at least containing some biological components). (...) In all of these cases, there seems to be a 'shared' or 'distributed' responsibility between robot designers, engineers, programmers, manufacturers, investors, sellers and users. None of these agents can be indicated as the ultimate source of action. At the same time, this solution tends to dilute the notion of responsibility altogether: if everybody has a part in the total responsibility, no one is fully responsible. This problem is known as the 'problem of the many hands'. (…) *Robots may be used for purposes intended by their designers, but they may also be used for a variety of other purposes, especially if their 'behaviour' can be 'hacked' or 'reprogrammed' by their end-users. Robots might have implications far beyond the intentions of their developers. It is impossible for roboticists to predict entirely how their work might affect society.*

[992] O Chatbot Tay acabou sendo desativado. Cf. Elle Hunt. Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter. The Guardian, 24 mai. 2016. Disponível em: <https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter>. Acesso em: 26 mai. 2017.

[993] Recentemente, "Alpha Go", uma inteligência artificial desenvolvida pelo Google, derrotou, pela segunda vez, o campeão mundial do jogo de tabuleiro chinês Go, considerado um dos jogos de estratégia mais difíceis já criados. Apenas para se ter uma dimensão da complexidade do jogo, o Go comporta cerca de 2.1×10^{170} posições possíveis em um tabuleiro, enquanto o Xadrez admite um número de posições legais que se encontra entre as ordens de grandeza 10^{43} e 10^{50}. A título de comparação, estima-se que em todo o universo visível não há mais do que 10^{90} prótons. Disponível

parâmetros claros de como se deve conduzir esse estudo, sob o ponto de vista da ética. A necessidade de se construir um *framework* regulatório para esse tipo de tecnologia vem sendo destacada por algumas iniciativas.

Nesse sentido, em janeiro de 2017 foi realizada uma conferência em Asilomar[994], CA, com o intuito de definir uma série de princípios para que o desenvolvimento de programas de Inteligência Artificial se dê de forma benéfica. Os 23 princípios são:

> *1) Research Goal: The goal of AI research should be to create not undirected intelligence, but beneficial intelligence.*
> *2) Research Funding: Investments in AI should be accompanied by funding for research on ensuring its beneficial use, including thorny questions in computer science, economics, law, ethics, and social studies, such as:*
> - *How can we make future AI systems highly robust, so that they do what we want without malfunctioning or getting hacked?*
> - *How can we grow our prosperity through automation while maintaining people's resources and purpose?*
> - *How can we update our legal systems to be more fair and efficient, to keep pace with AI, and to manage the risks associated with AI?*
> - *What set of values should AI be aligned with, and what legal and ethical status should it have?*
>
> *3) Science-Policy Link: There should be constructive and healthy exchange between AI researchers and policy-makers.*
> *4) Research Culture: A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI.*
> *5) Race Avoidance: Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards.*
> *6) Safety: AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.*
> *7) Failure Transparency: If an AI system causes harm, it should be possible to ascertain why.*
> *8) Judicial Transparency: Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.*
> *9) Responsibility: Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.*
> *10) Value Alignment: Highly autonomous AI systems should be designed so that their goals and behaviors can be assured to align with human values throughout their operation.*
> *11) Human Values: AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.*
> *12) Personal Privacy: People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data.*

em: <http://economia.ig.com.br/2017-11-06/deepmind-inteligencia-artificial.html>. Acesso em: 25 mai. 2017.

[994] Disponível em: <https://futureoflife.org/ai-principles/>. Acesso em: 25 mai. 2017.

13) Liberty and Privacy: The application of AI to personal data must not unreasonably curtail people's real or perceived liberty.
14) Shared Benefit: AI technologies should benefit and empower as many people as possible.
15) Shared Prosperity: The economic prosperity created by AI should be shared broadly, to benefit all of humanity.
16) Human Control: Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.
17) Non-subversion: The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.
18) AI Arms Race: An arms race in lethal autonomous weapons should be avoided.
19) Capability Caution: There being no consensus, we should avoid strong assumptions regarding upper limits on future AI capabilities.
20) Importance: Advanced AI could represent a profound change in the history of life on Earth, and should be planned for and managed with commensurate care and resources.
21) Risks: Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact.
22) Recursive Self-Improvement: AI systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.
23) Common Good: Superintelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization."[995]

[995] Tradução livre do autor: 1) Objetivo da pesquisa: o objetivo da pesquisa da AI deve ser criar inteligência não-direcionada, mas inteligência benéfica. 2) Financiamento da pesquisa: os investimentos em AI devem ser acompanhados de financiamento para pesquisas sobre o seu uso benéfico, incluindo questões espinhosas em ciência da computação, economia, direito, ética e estudos sociais, tais como: como podemos tornar os sistemas de AI futuros altamente robustos , de modo que eles façam o que queremos, sem funcionar mal ou ser pirateados? Como podemos aumentar a nossa prosperidade através da automação, mantendo os recursos e o propósito das pessoas? Como podemos atualizar nossos sistemas legais para serem mais justos e eficientes, para acompanhar a AI e gerenciar os riscos associados à AI? Qual o conjunto de valores com o qual AI deve ser alinhado, e que status legal e ético deve ter? 3) Link Ciência-Política: deve haver um intercâmbio construtivo e saudável entre pesquisadores de AI e decisores políticos. 4) Cultura de pesquisa: uma cultura de cooperação, confiança e transparência deve ser promovida entre pesquisadores e desenvolvedores de AI. 5) Prevenção de corrida: as equipes que desenvolvem sistemas de AI devem cooperar ativamente para evitar esquemas nas normas de segurança. 6) Segurança: os sistemas AI devem ser seguros e seguros ao longo de sua vida útil, e de forma verificável, quando aplicável e viável. 7) Transparência de falha: se um sistema de AI causar danos, deve ser possível verificar o porquê. 8) Transparência judiciária: qualquer envolvimento de um sistema autônomo na tomada de decisões judiciais deve fornecer uma explicação satisfatória e auditável por uma autoridade humana competente. 9) Responsabilidade: designers e construtores de sistemas avançados de AI são partes interessadas nas implicações morais de seu uso, uso indevido e ações, com a responsabilidade e a oportunidade de moldar essas implicações. 10) Alinhamento do valor: os sistemas AL altamente autônomos devem ser projetados para que seus objetivos e comportamentos possam ser assegurados para se alinhar com os valores humanos ao longo de sua operação. 11) Valores humanos: os sistemas de AI devem ser projetados e operados de forma a serem compatíveis com ideais de dignidade humana, direitos, liberdades e diversidade cultural. 12) Privacidade pessoal: as pessoas devem ter o direito de acessar, gerenciar e controlar os dados que geram, dado o poder dos sistemas AI para analisar e utilizar esses dados. 13) Liberdade e Privacidade: A aplicação de AI aos dados pessoais não deve restringir

Conforme se extrai da parte de responsabilidade do texto (9)[996], os designers de sistemas avançados de AI devem ser considerados partes interessadas nas implicações morais de seu uso, bem como no caso de uso indevido da Coisa e de ações autônomas danosas, recaindo sobre eles a responsabilidade e a oportunidade de moldar essas implicações.

Aliado a isso, deve ser considerada também responsabilidade do designer a preocupação com a garantia de valores como privacidade, segurança e ética no design dos artefatos. Isso visa evitar ao máximo problemas *a posteriori*, levando em conta sempre o que está dentro da esfera de controle e influência do designer. Extrai-se daí o desafio de se pensar, portanto, em um "design sensível a valores". Como exemplo podemos citar os comandos de: "*privacy by design*", "*security by design*" e "*ethics by design*", que serão melhor explorados no item seguinte.

Precisamos também pensar no grau de autonomia que pode razoavelmente ser deixado para a máquina e onde o controle humano substancial deve ser mantido. O esquema contido na tabela abaixo, produzida no estudo da UNESCO[997], traz parâmetros importantes que nos ajudam a pensar sobre essas questões tentando identicar as diferentes agências envolvidas. Embora a estrutura proposta seja simples, sua implementação em termos de atribuição de

injustificadamente a liberdade real ou percebida das pessoas. 14) Benefício compartilhado: as tecnologias AI devem beneficiar e capacitar o maior número de pessoas possível. 15) Prosperidade compartilhada: a prosperidade econômica criada pela IA deve ser compartilhada de forma ampla, para beneficiar toda a humanidade. 16) Controle humano: os seres humanos devem escolher como e se delegar decisões aos sistemas de AI, para atingir objetivos humanos escolhidos. 17) Não-subversão: o poder conferido pelo controle de sistemas de IA altamente avançados deve respeitar e melhorar, em vez de subverter, os processos sociais e cívicos nos quais depende a saúde da sociedade. 18) AI Arms Race: uma corrida armamentista em armas autônomas letais deve ser evitada. 19) Capacidade Cuidado: Não havendo consenso, devemos evitar fortes pressupostos em relação aos limites superiores das capacidades de AI futuras. 20) Importância: A AI avançada poderia representar uma mudança profunda na história da vida na Terra e deveria ser planejada e gerenciada com recursos e recursos compatíveis. 21) Riscos: os riscos provocados pelos sistemas de AI, especialmente riscos catastróficos ou existenciais, devem ser sujeitos a planejamento e mitigação de esforços proporcionais ao impacto esperado. 22) Auto-aperfeiçoamento recursivo: sistemas de AI concebidos para auto-melhorar recursivamente ou auto-replicar de uma forma que pode levar a uma qualidade ou quantidade cada vez maior, devem estar sujeitos a medidas rigorosas de segurança e controle. 23) Bom comum: a superinteligência só deve ser desenvolvida ao serviço de ideais éticos amplamente compartilhados e em benefício de toda a humanidade e não de um estado ou organização.

[996] No original: *Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications*.

[997] Disponível em: <http://unesdoc.unesco.org/images/0025/002539/253952E.pdf>. Acesso em: 25 mai. 2017.

responsabilidade e regulação do uso é complexa e desafiadora - para cientistas e engenheiros, decisores políticos e eticistas.

Adotando um caminho alternativo, em 16 de fevereiro de 2017, o Parlamento Europeu editou uma resolução com recomendações da Comissão Europeia de regras de *civil law* em robótica (2015/2103(INL)). Dentre outras questões, o documento advoga pela criação de uma agência Europeia para robótica e inteligência artificial, para prover a expertise técnica, ética e regulatória necessária.[998]

O Parlamento Europeu propôs, ainda, considerar a introdução de um status jurídico específico para robôs inteligentes a longo prazo, bem como a criação de um sistema de seguro ou de fundo compensatório, com o objetivo de criar um sistema de proteção para o emprego de máquinas inteligentes.

Quanto ao status jurídico legal que poderia ser conferido a esses agentes, a resolução utiliza a expressão "pessoa eletrônica" ou "*e-person*". Além disso, diante do cenário de desconexão entre ética e tecnologia, a diretriz europeia acertadamente afirma que a dignidade, em um viés deontológico, deve estar no centro de uma nova ética digital.

A atribuição de personalidade[999] a robôs inteligentes parece correta e coerente inclusive com o ganho de autonomia[1000] das Coisas inteligentes.[1001]

---

[998] Disponível em: <http://www.cms-lawnow.com/ealerts/2017/04/do-robots-have-rights-the-european-parliament-addresses-artificial-intelligence-and-robotics>. Acesso em: 26 set. 2017.

[999] As características mais utilizadas para o embasamento da personalidade humana são: consciência; racionalidade; autonomia (*self motivated activity*); capacidade de comunicação e; auto-consciência (*self-awereness*). Outro critério social possível é ser considerado uma pessoa sempre que a sociedade assim o reconhecer (podemos aplicar inclusive a teoria habermasiana aqui, através de um processo deliberativo na esfera pública). Outros teóricos acreditam que a característica fundamental para atribuição de personalidade é a sensciência que significa a capacidade de sentir prazer e dor. Segundo Juliana de Andrade, baseando-se na teoria dos 'entes despersonalizados' defendida por Daniel Lourenço: "Em primeiro lugar, para nós, como visto, o animal não humano é um ser senciente, assim como o homem, e por isso deve ter o seu interesse em não sofrer igualmente tutelado pelo nosso ordenamento jurídico – o que, de fato, já foi feito pela Constituição Federal de 1988, ao proibir a prática de atos cruéis contra os animais não humanos. Desse modo, a legislação civilista precisa se adequar a essa realidade e reconhecer a condição de sujeito de direito do animal não humano." Além disso, o direito já rompeu uma barreira importante com relação à atribuição de personalidade ao conceder personalidade também a pessoas jurídicas. LOURENÇO, Daniel Braga. Direito dos animais: fundamentação e novas perspectivas. Porto Alegre: Sergio Antonio Fabris. Ed., 2008, p. 141. A natureza jurídica dos animais: rompendo com a tradição antropocêntrica. ANDRADE, Juliana. A natureza jurídica dos animais: rompendo com a tradição antropocêntrica. Disponivel em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=16684#_ftn62>. Acesso em: 25 mai. 2017.

[1000] A moral kantiana estabelece o seu fundamento na autonomia, para cuja efetivação subentende-se a necessidade da liberdade e caracteriza-se pela capacidade de pensar e agir por si mesmo.

Nesse sentido, conforme sustenta o professor da GeorgeTown University, David Vladeck:[1002]

> Uma solução seria conceituar novamente essas máquinas autônomas e inteligentes como entidades com o status de "pessoa", de acordo com a lei. Conferir "personalidade" a essas máquinas resolveria a questão da agência; as máquinas se tornariam atores em seu próprio direito, e, juntamente com o novo estatuto jurídico, viriam novos encargos legais, incluindo o ônus do auto-seguro. Esta é uma forma diferente de difusão de custos do que a concentração apenas nos criadores do veículo, e pode ter a virtude de exigir que um público mais amplo - incluindo o proprietário do veículo - participe do financiamento do *pool* de seguros, o que também pode ser mais justo.[1003]

A atribuição de direitos a robôs e a criação de uma personalidade própria, não chega a ser uma novidade. Na doutrina jurídica brasileira, Marco Aurélio de Castro em sua obra intitulada "Direito e Pós-humanidade: quando os robôs serão sujeitos de direitos" de 2009, já apontava nessa direção.[1004]

Em concordância com os ensinamentos de Lehman-Wilzig, Castro defende que não há um significado claro para o conceito de "pessoa", portanto não se pode

---

defende que todo o ser humano, à medida que ele é racional, pode alcançar a autonomia, isto é, ele mesmo dar a direção para a sua vida. Para essa efetivação, basta que tenha coragem para fazer uso de seu próprio entendimento, isto é, de pensar por si mesmo. É necessário lembrar, no entanto, que para o ser humano se auto-determinar, ele necessita viver em comunidade. Habermas complementa essa concepção inicial kantiana. Nas palavras de Haide Maria Hupffer: "Habermas avança indicando que autonomia também deve ser entendida como princípio da democracia. Para Habermas a moralidade é um processo de argumentação entre uma sociedade livre e autônoma. O autor busca reconstruir o nexo interno entre soberania popular e direitos humanos introduzindo o princípio do discurso. A partir da diferenciação entre moral e direito, Habermas introduz seu modo de interpretar o conceito de autonomia, apoiado no princípio do discurso, ou seja, a autonomia está na liberdade comunicativa, pressuposta no agir que se orienta pelo entendimento mútuo. Para que uma norma seja universal é necessário o consenso, isto é, para que possamos nos sentir destinatário de direitos, é necessário o entendimento enquanto autores de direito. A importância de trazer Habermas ao texto pode ser sustentada pelo fato de que, em Habermas a moralidade é fruto de um processo argumentativo entre seres livres e autônomos." Disponível em: <http://www.anima-opet.com.br/pdf/anima5-Seleta-Externa/Haide-Maria-Hupffer.pdf>. Acesso em: 29 set. 2017. Immanuel Kant. Resposta à pergunta: O que é o Esclarecimento? 1783.

[1001] Além de estar consonante com a visão de autonomia kantiana, a diretriz europeia claramente se vale de uma visão deontológica e não utilitarista para a regulação de robôs inteligentes.

[1002] VLADECK, David. *Machines Without Principals:* Liability Rules And Artificial Intelligence. Disponivel em: <https://perma.cc/EJ5M-YMCJ>. Acesso em: 25 mai. 2017.

[1003] Tradução livre do autor. No original: *One solution would be to reconceptualize these autonomous, intelligent machines as entities with the status of a "person" under the law. Conferring "personhood" on these machines would resolve the agency question; the machines become principals in their own right, and along with new legal status would come new legal burdens, including the burden of self-insurance. This is a different form of cost-spreading than focusing on the vehicle's creators, and it may have the virtue of necessitating that a broader audience—including the vehicle's owner—participate in funding the insurance pool, and that too may be more fair.*

[1004] CASTRO, Marco Aurélio. *Direito e Pós-humanidade: quando os robôs serão sujeitos de direitos*. Salvador: 2009.

arguir que ser pessoa é necessariamente ser-humano. Temos hoje o precedente inclusive de entidades empresariais enquadradas com status jurídico de pessoa.[1005] Castro defende então a possibilidade de artefatos se enquadrarem também nesse conceito, tendo em vista que um robô poderá realizar atividades antes encaradas como privativas de seres humanos como: predizer, escolher, aprender, compreender, interpretar, analisar, decidir, sentir[1006], entre outras capacidades e habilidades. Nas palavras de Castro:[1007]

> Descobertos os elementos que, reunidos ou isoladamente resultam na personalidade do indivíduo jurisdicizada, é lícito afirmar que, se outro ente for encontrado dotado desses mesmos elementos, a conclusão lógica é a de se atribuir o mesmo status jurídico de pessoa. (...) Cérebro e computador não se equivalem, o que pouco importa, pois, se a sua manifestação for um efeito ou ato inteligente, o que o causar haverá de ser inteligente, pois o que permanece no pensamento não pode ser de forma alguma avaliado, apenas seu resultado. O que acontece no interior de um computador, quando em funcionamento, muitas vezes é um mistério insondável, como ainda é o mistério do que ocorre no cérebro quando pensamos.

Tendo em vista as diferentes potencialidades das Coisas inteligentes, Marco Aurélio defende inclusive uma diferenciação análoga à distinção civil e penal baseada na capacidade humana. Portanto, somente Coisas inteligentes com as mesmas características humanas poderiam ser considerados absolutamente capazes. O que propõe é que se criem parâmetros ou patamares para que se tenha, sob a ótica jurídica, robôs incapazes (sem responsabilidade moral), relativamente capazes (monitorados e tutelados, cujas decisões mais críticas careçam de intervenção humana) ou plenos como os humanos adultos, sem restrições jurídicas.

[1005] O conceito jurídico de pessoa é mutável e está em constante evolução. Por exemplo, os afro-descendentes já foram excluídos dessa categoria, na época da escravatura. Portanto, não se pode relacionar o conceito jurídico de pessoa com o *Homo sapiens.* Em analogia, etimologicamente o termo robô significa trabalhador forçado. Nada obsta para que migrem também para a categoria de ente titular de direitos e obrigações, uma vez que desempenhem as mesmas ações que os seres humanos. CASTRO, Marco Aurélio. *Direito e Pós-humanidade: quando os robôs serão sujeitos de direitos*. Salvador: 2009.

[1006] Há que se fazer aqui uma ressalva pois ainda que os robôs consigam sentir e demonstrar emoções como se fossem senscientes, questiona-se a autenticidade dessas reações tendo em vista que não seriam genuínas, mas no máximo uma representação (ou emulação), análogo a atores humanos quando simulam em uma peça de teatro, por exemplo, sentimentos em papéis determinados, não sendo considerado por muitos como algo genuino. Por conta disso, o jus-filósofo italiano Ugo pagallo denomina isso de 'autonomia artificial'.

[1007] CASTRO, Marco Aurélio. Direito e Pós-humanidade: quando os robôs serão sujeitos de direitos. Salvador: 2009.

Uma das características importantes de se levar em consideração é a velocidade de aprendizado e a evolução individual do robô (baseados no processamento de dados), que pode representar em alguns casos a inviabilidade de um processo educativo, limitando, portanto, sua responsabilidade moral e jurídica.

Mas como se poderia castigar um robô? Não poderia ser tão simples quanto 'puxar a tomada'. Nesse caso, abrem-se duas saídas: reabilitação e indenização. A primeira, envolveria a reprogramação do robô culpado. A segunda, seria obrigar o mesmo a compensar a vítima pelo dano causado.

Reside justamente aí a pertinência da resolução europeia. A proposta de atribuição de um novo tipo de personalidade (eletrônica), considerando características próprias das Coisas inteligentes, conjugada com a ideia de um seguro obrigatório ou fundo compensatório pode ser um primeiro passo importante.

A nova proposta europeia reflete uma resposta prática mais célere para o problema mencionado anteriormente de "irresponsabilidade distribuída"[1008], que ocorre quando não se encontra uma conexão clara entre um agente e o dano gerado.

Caitlin Sampaio Mulholland abordou de forma notável a problemática da responsabilidade distribuída/difusa em sua tese sobre presunção de causalidade. Em arejada análise, Caitlin Mulholland enfrenta o cenário de falta de clareza do nexo causal entre os agentes reforçando o conceito de causalidade alternativa. Segundo Mulholland, diante da exististência de um único nexo causal que não pode ser identificado de forma direta, podemos atrbuir a sua presunção ao grupo econômico como um todo, possibilitando a reparação dos danos causados através da facilitação do ônus probatório para a vítima.

No entanto, quando pensamos nos danos ocorridos dentro de sistemas sociotécnicos complexos, temos uma aplicação de nexo causal e de responsabilidade jurídica ainda mais desafiadora. Isso porque estamos falando muitas vezes da ação causada por um somatório de agências de seres humanos, instituições e coisas inteligentes com autonomia e poder de agência próprios. Nesse caso, o foco no grupo econômico, apesar de conseguir responder a diversos

[1008] Esse fenômeno jurídico é também denominado por outros autores como "*problem of the many hands*" ou "*accountability gap*".

casos de dano, pode não ser suficiente para a atribuição justa de responsabilidade na era de IoT e de inteligência artificial forte.[1009]

Portanto, como uma resposta pragmática diante desse cenário de incerteza e falta de adequação jurídica, a proposta europeia sugere que, em caso de dano, a pessoa lesada pode lançar mão do seguro ou ser ressarcida através do fundo compensatório.[1010]

Vale destacar a parte de responsabilidade como consta da Resolução:[1011] [1012]

> *Liability*
> *31. Calls on the Commission, when carrying out an impact assessment of its future legislative instrument, to explore the implications of all possible legal solutions, such as:*
> *a) establishing a compulsory insurance scheme whereby, similarly to what already happens with cars, producers or owners of robots would be required to take out insurance cover for the damage potentially caused by their robots;*
> *b) ensuring that a compensation fund would not only serve the purpose of guaranteeing compensation if the damage caused by a robot was not covered by an insurance – which would in any case remain its primary goal – but also that of allowing various financial operations in the interests of the robot, such as investments, donations or payments made to smart autonomous robots for their services, which could be transferred to the fund;*
> *c) allowing the manufacturer, the programmer, the owner or the user to benefit from limited liability insofar as smart autonomous robots would be endowed with a compensation fund – to which all parties could contribute in varying proportions – and damage to property could only be claimed for within the limits of that fund, other types of damage not being subject to such limits;*
> *d) deciding whether to create a general fund for all smart autonomous robots or to create an individual fund for each and every robot category, and whether a*

[1009] MULHOLLAND, Caitlin Sampaio. A responsabilidade civil por presunção de causalidade. Rio de Janeiro: GZ, 2010.

[1010] Ainda é uma questão em aberto o tipo de seguro que deve ser aplicado ao caso de robôs inteligentes e quais agentes e instituições deveriam arcar com esse ônus. O relatório recente da União Europeia (2015/2103(INL)) editou recomendações sobre o assunto, propondo não apenas um registro obrigatório, como também a criação de seguros e fundos. Segundo o parlamento europeu, os seguros poderiam ser assumidos tanto pelo consumidor, quanto pela empresa, em um modelo similar àqueles utilizados pelos seguros de automóveis que existem atualmente. Já o fundo poderia ser geral (para todos os robôs autônomos) ou individual (para cada categoria de robô), composto por taxas pagas no momento de colocação da máquina em mercado, e/ou contribuições pagas periodicamente durante todo o tempo de vida dos robôs. Vale ressaltar que, nesse caso, as empresas seriam responsáveis por arcar com esse ônus. Apesar dessa proposta, entretanto, o tópico continua em debate aberto, comportando novas alternativas e modelos mais interessantes – como fundos privados, registros específicos, dentre outras possibilidades -, que não serão objeto de análise profunda nesta tese.

[1011] Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//PT>. Acesso em: 25 mai. 2017.

[1012] Disponível em: <http://img.rtp.pt/icm/noticias/docs/6c/6c3203f10cc5377801aae1c0d1b8ce13_467b87e0a1eaa0377cb70477245debc3.pdf>. Acesso em: 25 mai. 2017.

contribution should be paid as a one-off fee when placing the robot on the market or whether periodic contributions should be paid during the lifetime of the robot; e) ensuring that the link between a robot and its fund would be made visible by an individual registration number appearing in a specific EU register, which would allow anyone interacting with the robot to be informed about the nature of the f) creating a specific legal status for robots, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons with specific rights and obligations, including that of making good any damage they may cause, and applying electronic personality to cases where robots make smart autonomous decisions or otherwise interact with third parties independently;[1013][1014]

No entanto, esse passo deve ser acompanhado de perto por um contínuo debate sobre os princípios éticos que devem nortear esse tipo de artefatos técnicos, bem como uma adequada governança de todos os dados utilizados na construção e desenvolvimento destes agentes.

[1013] Vide: European Parliament. Committee on Legal Affairs DRAFT REPORT with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//PT>. Acesso em: 25 mai. 2017.

[1014] Tradução livre do autor: Responsabilidade. 31. Solicita à Comissão que, ao realizar uma avaliação de impacto do seu futuro instrumento legislativo, explore as implicações de todas as possíveis soluções jurídicas, tais como: a) estabelecer um regime de seguro obrigatório pelo qual, de forma semelhante ao que já acontece com os automóveis, os produtores ou os proprietários de robôs seriam obrigados a retirar a cobertura do seguro pelos danos potencialmente causados por seus robôs; b) garantir que um fundo de compensação não só servisse para garantir a compensação se o dano causado por um robô não fosse coberto por um seguro - o que, em qualquer caso, continuaria sendo o principal objetivo -, mas também o de permitir diversas operações financeiras na interesses do robô, tais como investimentos, doações ou pagamentos feitos a robôs autônomos inteligentes para seus serviços, que poderiam ser transferidos para o fundo; c) permitindo que o fabricante, o programador, o proprietário ou o usuário se beneficiem de responsabilidade limitada na medida em que os robôs autônomos inteligentes seriam dotados de um fundo de compensação - ao qual todas as partes poderiam contribuir em proporções variáveis - e danos à propriedade só poderiam ser reivindicados dentro dos limites desse fundo, outros tipos de danos não estão sujeitos a tais limites; d) decidir se deve criar um fundo geral para todos os robôs inteligentes autônomos ou criar um fundo individual para cada categoria de robôs e se uma contribuição deve ser paga como uma taxa única ao colocar o robô no mercado ou se periódico as contribuições devem ser pagas durante a vida útil do robô; e) garantir que o link entre um robô e seu fundo fique visível por um número de registro individual que apareça em um registro específico da UE, o que permitiria que qualquer pessoa que interagisse com o robô seja informada sobre a natureza da f) criando um direito legal específico status para robôs, para que, pelo menos, os robôs autônomos mais sofisticados possam ser estabelecidos como tendo o status de pessoas eletrônicas com direitos e obrigações específicos, incluindo o de reparar os danos que possam causar e a aplicação de personalidade eletrônica aos casos em que os robôs são inteligentes decisões autônomas ou de outra forma interagir com terceiros independentemente;

Ao tratar da importância de uma discussão profunda na sociedade sobre a criação de nova personalidade e regulação destas novas tecnologias, Lawrence B. Solum atesta:[1015]

> Nossas teorias de personalidade não podem fornecer um quadro a priori para as profundezas que envolvem as fronteiras de status. Uma resposta à questão sobre se deve ser concedida alguma forma de personalidade jurídica às inteligências artificiais não pode ser dada até que nossa forma de vida torne urgente essa questão. Enquanto nossos encontros diários com inteligência artificial aumentam o debate sobre a personalidade, eles podem mudar nossa perspectiva sobre como a questão deve ser respondida. E assim deve ser com as perguntas difíceis que enfrentamos hoje. Debates sobre fronteiras de status – como aborto, término do tratamento médico e direitos dos animais - não serão resolvidos por teorias profundas ou por intuições geradas por situações imaginativas e hipotéticas. É claro que muitos de nós acreditamos em teorias profundas; aderimos a uma variedade abrangente de doutrinas filosóficas ou religiosas. Mas, em uma sociedade moderna e pluralista, o desacordo sobre questões finais é profundo e persistente. A resolução de casos difíceis nas esferas política e judicial requer o uso da razão pública. Não temos uma alternativa realista senão buscar um compromisso baseado em princípios, e em nosso patrimônio compartilhado de tolerância e respeito. Se não há um terreno comum para construir uma teoria da personalidade que resolva um caso difícil, então os juízes devem recair sobre o princípio do respeito pelos direitos daqueles que mutuamente se reconhecem como cidadãos.[1016]

Do ponto de vista jurídico, é fundamental termos em mente também a nova natureza do controle e responsabilidade difusa, potencialmente dispersa no espaço, no tempo e na agência dos diversos actantes atuantes na esfera pública. Precisamos pensar sobre o contexto em que os pressupostos sobre a responsabilidade estão sendo feitos. A questão que nos é apresentada não é

[1015] LAWRENCE B. Solum, Legal Personhood for Artificial Intelligences, 70 N.C. L. Rev. 1231 (1992). Available at: Disponível em: <http://scholarship.law.unc.edu/nclr/vol70/iss4/4>. Acesso em: 25 mai. 2017.

[1016] Tradução livre do autor. No original: *Our theories of personhood cannot provide an a priori chart for the deep waters at the borderlines of status. An answer to the question whether artificial intelligences should be granted some form of legal personhood cannot be given until our form of life gives the question urgency. But when our daily encounters with artificial intelligence do raise the question of personhood, they may change our perspective about how the question is to be answered. And so it must be with the hard questions we face today. Debates about the borderlines of status-about abortion, about the termination of medical treatment, and about rights for animals-will not be resolved by deep theories or the intuitions generated by wildly imaginative hypotheticals. Of course, many of us do believe in deep theories; we subscribe to a variety of comprehensive philosophical or religious doctrines. But in a modem, pluralist society, the disagreement about ultimate questions is profound and persistent. Resolution of hard cases in the political and judicial spheres requires the use of public reason. We have no realistic alternative but to seek principled compromise based on our shared heritage of toleration and respect. If there is no common ground on which to build a theory of personhood that resolves a hard case, then judges must fall back on the principle of respect for the rights of those who mutually recognize one another as fellow citizens.*

somente como tornar os agentes computacionais responsáveis, mas sim como aplicar a responsabilidade de forma justa. Devemos pensar então em uma "responsabilidade compartilhada" entre os diferentes actantes atuantes na rede sociotecnica e suas esferas de controle e influência sobre as situações e sobre os demais agentes.

Porém, ainda estamos longe de obter um consenso razoável[1017] sobre o estabelecimento dos parâmetros éticos adequados para o desenvolvimento de algoritmos e demais Coisas inteligentes. Conforme defendido neste trabalho, esses agentes são capazes de influenciar as relações entre as pessoas, moldando comportamentos e visões de mundo, especialmente quando parte do seu funcionamento goza de alta complexidade tecnológica e autonomia, como ocorre no caso dos sistemas de Inteligência Artificial com capacidade de raciocínio e de aprendizagem segundo técnicas de *deep learning* em redes neurais [1018] artificiais[1019].

É perceptível que esses elementos estão exercendo cada vez mais influência no modo como nos organizamos em sociedade e, por isso, o avanço científico e jurídico não pode andar apartado da ética. O papel do direito neste contexto deve sofrer releituras. Conforme veremos no item seguinte, a regulação jurídica, construída democraticamente na esfera pública, deve fornecer a arquitetura adequada para proporcionar a construção dos canais éticos apropriados para que o fluxo de dados e de ações não-humanas possam escoar dentro dos limites ético-jurídicos pautados por uma visão deontológica.

3.5
Direito como Meta-Tecnologia: O Desafio do *Rule Of Law* em um Mundo Tecno-Regulado

[1017] Defende-se neste trabalho que o consenso seja construído nos moldes propostos por Jurgen Habermas através de embates dialógios na esfera pública.
[1018] *Artificial Neural Networks* (ANN)representam uma rede de vários processadores simples – "neurônios" – em que cada um possui, geralmente, uma memória local. ANN é um sistema adaptativo complexo, de modo que ele pode alterar sua estrutura interna com base nas informações que passam por ele.
[1019] AMARAL, Gustavo Rick. Uma dose de pragmatismo para as epistemologias contemporâneas: Latour e o parlamento das coisas. *Teccogs: Revista Digital de Tecnologias Cognitivas*, São Paulo, n. 12, p. 94, jul-dez. 2015.

O filósofo e eticista italiano Luciano Floridi recentemente declarou: "Estamos entrando na Era do Design e devemos fazer de tudo para que seja a Era do 'bom' design".[1020] Anos antes, na obra Code 2.0, o professor de Harvard e especialista em tecnologia, Lawrence Lessig, já havia decretado '*Code is Law'*[1021]. Ambas as declarações possuem uma mesma linha de argumentação: somos hoje regulados e influenciados pela arquitetura das plataformas digitais (pelo seu *design*), tanto quanto por outras regulações como, por exemplo, o Direito, as normas sociais e a economia.

Atrelado à essa preocupação, devemos compreender melhor, ainda, a interação entre humanos e Coisas (artefatos técnicos), considerando suas características ontológicas, visto que estas são dotadas de função e plano de uso atribuídos nas fases de design e desenvolvimento, gerando a elas uma moralidade intrínseca que nos influencia e condiciona. Esses elementos têm gerado impactos cada vez maiores no âmbito social e político, conforme sustentado ao longo deste trabalho.

Além de termos hoje agentes não-humanos atuando na esfera pública conectada, a situação fica ainda mais complexa quando levamos em consideração as chamadas 'ações tecnológicas'. Por serem muitas vezes imprevisíveis, produzidas nos complexos sistemas sociotécnicos que englobam a soma de diversas ações de actantes humanos e não-humanos, as ações tecnológicas colocam em cheque as teorias jurídicas relacionadas à vontade e à responsabilidade.

Nesse novo cenário, constituído por um mundo de dados processados por diferentes tipos de actantes, algoritmos e demais sistemas dotados de *Machine learning* conseguem influenciar a esfera pública e políticas públicas, desempenhando um novo papel na indução de comportamentos e tomadas de decisão.[1022]

Apesar deste ser por si só um cenário novo e desafiador envolvendo a moralidade das Coisas, nossa 'relacionalidade' com elas e seus efeitos democráticos, devemos também entender o papel que o Direito deve

[1020] FLORIDI, Luciano. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality.* Oxford Press. 2016.
[1021] Code Is Law: On Liberty in Cyberspace. Lawrence Lessig. Harvard Magazine. Disponível em: <http://harvardmagazine.com/2000/01/code-is-law-html> Acesso em: 24 mai. 2017.
[1022] Disponível em: <https://perma.cc/C64Z-JJMD>. Acesso em: 24 mai. 2017.

desempenhar nesse contexto, como ferramenta regulatória e indutora de comportamentos, visando a paz social.

Segundo o teórico italiano de Direito e Tecnologia, Ugo Pagallo:[1023]

> No entanto, há uma diferença crucial entre o debate jurídico sobre a automação da década de 1890 e as discussões atuais sobre processamento automatizado. O salto tecnológico diz respeito à "lógica envolvida" nesse processamento automatizado. Este último considera cada vez mais uma classe particular de algoritmos que aumentam ou substituem a análise e a tomada de decisões pelos seres humanos, como ocorre com a disciplina da aprendizagem por máquinas, ou seja, algoritmos capazes de definir ou modificar as regras de tomada de decisão de forma autônoma. O segundo passo da nossa fenomenologia tem, portanto, a ver com o campo da AI e mais particularmente, com a mudança crucial da automação para a autonomia artificial.[1024]

Para Pagallo, estamos vivenciando hoje um cenário de mercantilização de dados pessoais que trafegam online e de forte tecno-regulação, sem que haja um balizamento ético-jurídico satisfatório para a proteção dos direitos constitucionais.[1025]

Apesar de regulações da Internet como o Marco Civil no Brasil tentarem valorizar o potencial da Internet e regular práticas que busquem proteger direitos constitucionais, a autoregulação tecnológica baseada no *design* do código[1026] simplesmente sobrepõe a regulação pelo Direito, subvertendo a tradicional lógica do "dever ser" típica do Estado de Direito, que salvaguarda o livre-arbítrio dos indivíduos, e estabelece uma lógica de "pode / não pode", sem deixar nenhuma alternativa de ação para cidadãos ou Governos.[1027] [1028]

[1023] PAGALLO, Ugo. *The laws of robots:* crimes, contracts, and torts. 2013.

[1024] Tradução livre do autor. No original: *There is however a crucial difference between the legal debate on automation from the 1890s and current discussions on automated processing. The technological leap concerns the "logic involved" in such automated processing. The latter increasingly regards a particular class of algorithms that either augment or replace analysis and decisionmaking by humans, as occurs with the discipline of machine learning, i.e. algorithms capable to define or modify decision-making rules autonomously. The second step of our phenomenology has thus to do with the field of AI and more particularly, with the crucial shift from automation to artificial autonomy.*

[1025] PAGALLO, Ugo. The laws of robots: crimes, contracts, and torts. 2013.

[1026] "*The expression "code design" here refers to the architecture of technology encompassing not only software though algorithmic design but also hardware architecture, as stated by Lawrence Lessig. "This regulator is code--the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced.*" Code Is Law: On Liberty in Cyberspace. Lawrence Lessig. Harvard Magazine. Disponível em: <http://harvardmagazine.com/2000/01/code-is-law-html>. Acesso em: 24 mai. 2017.

[1027] PAGALLO, Ugo and BAYAMLIOĞLU, Emre. *On the legal implications of regulation by technology:* of law and things. 2015.

[1028] A regulação de Coisas e plataformas digitais por algoritmos só permitem ao usuário realizar o que está programado. Além disso, quando se trata de provedor de conteúdo, este muitas vezes

Segundo Pagallo:[10291030]

> Onde instrumentos não normativos dominam o ambiente regulatório, parece que estamos sujeitos às regras da tecnologia e não ao Estado de Direito. Pode ser hora de perceber o fato de que o aumento da eficiência nem sempre resulta em soluções eficazes. "Para evitar nos tornarmos meramente um recurso cognitivo para estes ambientes nós devemos perceber como eles estão nos antecipando". Em um ambiente tecno-regulatório, as regras já não incorporam as políticas nas quais se baseiam, mas simplesmente as ditam. O direito e a política não operam como dois axiomas exclusivos, a saber, a política é o campo das relações de poder e das contestações; e o direito é a esfera da verdade e da justiça governada pelo Estado de Direito. A tecno-regulação sinaliza o fim de nossa capacidade de raciocinar contra e resistir, e assim pode resultar em um desvio maior dos valores que nos tornam "humanos".

No plano das redes sociais, por exemplo, o mecanismo de tecno-regulação utilizado pelo Youtube através do sistema de ID de conteúdo[1031] (*content ID*), coloca em risco a cultura brasileira do remix oriunda das expressões do Funk[1032] e do Tecnobrega[1033]. Isso se dá por meio do bloqueio automático realizado pelo website a qualquer vídeo que contenha conteúdo alheio protegido por *copyright,* o que representa uma censura prévia, sem uma adequada ponderação de princípios.

Em outro exemplo, o algoritmo do Facebook, ao tentar filtrar expressões pornográficas, recentemente censurou um post do Ministério da Cultura do Brasil (publicado através de seu perfil oficial do Facebook) com uma fotografia retratando duas nativas brasileiras. A foto em domínio público foi postada como parte do lançamento de um novo site em parceria com a Fundação da Biblioteca

---

realiza filtragens e remoções automáticas e invisíveis, executando por vezes censuras ilegítimas, desmotivadas e sem prestar qualquer informação ao consumidor. Esta prática ocorre diariamente, sem que as empresas de tecnologia sofram qualquer penalidade, uma vez que não existe uma regulação pelo Direito que os obrigue expressamente a qualquer destes deveres perante os consumidores.

[1029] PAGALLO, Ugo and BAYAMLIOĞLU, Emre. 2015, op.cit.

[1030] Tradução livre do autor. No original: *Where non-normative instruments dominate the regulatory environment, we seem to be subject to the rule of technology rather than the rule of law. It may be time to realise the fact that increase in efficiency do not always result with effective solutions. To prevent becoming merely the cognitive resource for these environments we must figure out how they are anticipating us. In a techno-regulatory setting, rules no longer embody the politics that they are based on, but they simply dictate it. Law and politics do not operate as two exclusive axioms namely, politics is the field of power relations and contestations; and law is the sphere of truth and justice governed by the rule of law. Techno-regulation signals the demise of our capacity to reason against and resist, and thus it may result with a further deviation from the values that make us "human".*

[1031] Disponível em: <https://support.google.com/youtube/answer/2797370?hl=pt-BR>. Acesso em: 24 mai. 2017.

[1032] Disponível em: <https://en.wikipedia.org/wiki/Funk_carioca>. Acesso em: 24 mai. 2017.

[1033] Disponível em: <https://en.wikipedia.org/wiki/Tecno_brega>. Acesso em: 24 mai. 2017.

Nacional e o Instituto Moreira Salles, contendo, na coleção, cerca de duas mil imagens históricas dos séculos XIX e XX.

Dada a falta de transparência para a filtragem automática e a indiferença demonstrada pelo Facebook neste caso, o Ministro da Cultura brasileiro declarou publicamente que a censura privada algorítimica era abusiva e violava os direitos de soberania e de acesso à cultura. Ainda, exigiu explicações adicionais por parte da empresa, ameaçando-a de um possível processo judicial.[1034]

Ambos os exemplos nos dão uma clara perspectiva de que a tecno-regulação já é uma prática bem estabelecida e vem sendo utilizada para atender exclusivamente a propósitos comerciais, sem qualquer preocupação em observar direitos constitucionais ou regulações específicas da Internet no Brasil como o Marco Civil da Internet, que declara enfaticamente a importância de se garantir a liberdade de expressão no ciberespaço.[1035]

Segundo Lawrence Lessig:[1036]

> A própria estrutura da Internet, isto é, o hardware e o software que compõem a estrutura técnica e os códigos que governam seu funcionamento, também são formas de regular o comportamento humano. Segundo o professor Lessig, a regulamentação através da estrutura é, às vezes, ainda mais eficaz do que outras formas mais familiares, como por exemplo, por meio da lei, da economia (mercado) e normas sociais. A própria estrutura dos sites nos torna reféns dos algoritmos, regulando nosso comportamento, bem como a lei, e criando sérios obstáculos ao acesso à informação, autonomia individual, privacidade e liberdade de expressão. [10371038]

O fato de que nos tornamos involuntariamente reféns dos algoritmos que nos inserem nessas bolhas, buscando a promessa de hiperconectividade e suas facilidades, caracteriza uma das mudanças contemporâneas mais drásticas e sutis, por ser muitas vezes imperceptível. Em um contexto tecno-regulado regido pela

---

[1034] Disponível em: <http://www.cultura.gov.br/noticias-destaques/-/asset_publisher/OiKX3xlR9iTn/content/id/1248553>. Acesso em: 24 mai. 2017.

[1035] On the legal implications of regulation by technology: of law and things. Ugo Pagallo (in press).

[1036] Code: Version 2.0. Lawrence Lessig. Basic Books, 2006.

[1037] A crítica à arquitetura algorítmica neste texto também pode ser expandida para arquitetura de *hardware.*

[1038] Tradução livre do autor. No original: *The very architecture of the Internet, that is, the hardware and software that make it up with technical structure and codes governing its functioning, are also ways to regulate human behavior. According to professor Lessig, regulation through architecture is sometimes even more effective than other more familiar forms such as law, economics (market) and social norms.[1038] The very architecture of the sites makes us hostage of the algorithms, regulating our behavior as well as the law and creating serious obstacles to access to information, individual autonomy, privacy and freedom of expression.*

lógica binária de algoritmos de "pode / não pode" (diferentemente do modelo de "dever ser" do sistema legal), o potencial democrático da esfera pública conectada e até mesmo a influência do *Rule of Law*[1039] (ou Estado de Direito)[1040] podem ser dramaticamente reduzidos.

O conceito de *Rule of Law* não é algo simples de se definir. O teórico Tom Bingham, em sua obra intitulada "*The Rule of Law*", faz um grande esforço para descrever a evolução do conceito e seu significado hoje. De acordo com Bingham, embora tenhamos uma idéia abstrata do que significa um "estado governado pelo direito" ("*law-governed state*") ou "as leis da terra" ("*the laws of the land*") e sua importância para as sociedades contemporâneas, é difícil atingir um consenso sobre um conceito único e fechado. [10411042]

No entanto, para os propósitos deste artigo, nos valemos da concepção de Bingham, considerando o Estado de Direito como o fundamento de uma sociedade civilizada que incorpora uma série de importantes idéias inter-relacionadas, da seguinte forma: primeiro é responsável por limitar o poder de o Estado. Um governo exerce sua autoridade através de leis publicamente divulgadas que são adotadas e executadas por um judiciário independente de acordo com procedimentos estabelecidos e aceitos. Em segundo lugar, ninguém está acima da lei; existe uma igualdade perante a lei. Em terceiro lugar, deve haver proteção dos direitos do indivíduo. Finalmente, a lei deve aplicar-se igualmente ao governo e aos cidadãos individuais. [1043] Embora Bingham considere o conceito como algo idealizado, o autor entende que é um ideal que vale a pena

---

[1039] *A expressão rule of law* possui origem na tradição anglo-saxônica, por vezes chamada também de "*legal state*", "*state of law*", "*state of justice*", "*state of rights*" ou "*state based on justice and integrity*". Na tradição *civil law* costuma-se denominar "Estado de Direito" ou "Estado Democrático de Direito". Nesse trabalho, nos valeremos dos termos como sinônimos em função das diferentes doutrinas utilizadas para embasar as teses aqui defendidas.

[1040] Usaremos ambos os termos como sinônimos nesse trabalho.

[1041] BINGHAM, Tom. *The Rule of Law*. Penguin, 2010.

[1042] Para José Joaquim Gomes Canotilho o princípio "*rule of law*" contém quatro dimensões bem nítidas: The rule of law significa, em primeiro lugar a obrigatoriedade da observância de um processo justo e legalmente regulado. Em segundo lugar, importa na proeminência das leis e costumes do país perante a discricionariedade do Estado. Por conseguinte, aponta para a sujeição de todos os atos do executivo à soberania do parlamento. E, Por fim, *rule of law* possui o sentido de igualdade de acesso aos tribunais por parte dos cidadãos a fim destes aí defenderem os seus direitos segundo os princípios de direito e perante qualquer entidade (indivíduos ou poderes públicos). Trata-se para Canotilho de um pressuposto lógico da Democracia, que se revela como verdadeira garantia contra o despotismo ao se firmar como suporte legal ao Estado Democrático de Direito. CANOTILHO, José Gomes. *Direito Constitucional e Teoria da Constituição*. Coimbra. Almedina. 1998. p.1177.

[1043] BINGHAM, Tom. *The Rule of Law*. Penguin, 2010.

ser buscado, enxergando a forte relação entre o Estado de Direito e a concretização dos direitos humanos e fundamentais.

Em 2004, o secretário-geral da ONU, Kofi Annan, forneceu uma definição[1044] compreensiva sobre o Estado de Direito, considerando esse "um princípio de governança em que todas as pessoas, instituições e entidades, públicas e privadas, incluindo o próprio Estado, são responsáveis perante leis promulgadas publicamente, igualmente aplicáveis, que são consistentes com as normas e padrões internacionais de direitos humanos". Segundo Annan, o Estado de Direito exige, ainda, medidas para garantir a adesão aos princípios de supremacia do direito, tais como igualdade e prestação de contas perante a lei, justiça na aplicação das normas, separação de poderes, participação na tomada de decisões, segurança jurídica, impedimento de arbitrariedade e transparência processual e legal".[1045]

Tendo em vista essa concepção de *Rule of Law*, podemos afirmar que existe hoje uma discrepância entre o papel que o Estado de Direito deveria representar nas sociedades contemporâneas e o recrudescimento da prática de tecno-regulação dos cidadãos realizada por empresas privadas na condução de suas plataformas digitais, englobando seus produtos e serviços oferecidos aos usuários. [1046]

A regulação algorítmica de dispositivos e plataformas restringe o usuário ao que já foi programado. Além disso, quando se trata de algoritmos e provedores de conteúdo, a filtragem e retirada de conteúdo são geralmente automatizadas, bastante invisíveis, e podem até mesmo cumprir censura ilegal (e desmotivada) sem as empresas serem responsabilizadas perante o usuário. Embora este tipo de prática ocorra diariamente, as empresas privadas de tecnologia não sofrem qualquer penalidade. É a tecno-regulação que se sobrepõe ao Estado Democrático de Direito.

[1044] Disponível em: <http://www.unrol.org/files/2004%20report.pdf>. Acesso em: 26 set. 2017.

[1045] No original: "a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency." Disponível em: <http://www.unrol.org/files/2004%20report.pdf>. Acesso em: 24 mai. 2017.

[1046] BINGHAM, Tom. *The Rule of Law*. Penguin, 2010.

Devemos compreender que o aumento da eficiência e a adoção acrítica de inovação tecnológica nem sempre resulta em soluções efetivas para a sociedade, conforme sustentamos no primeiro capítulo deste trabalho. Para evitar nos tornarmos meramente um recurso cognitivo e base de dados para os ambientes digitais, devemos descobrir como eles estão nos antecipando, interagindo conosco e nos regulando.

Em um cenário tecno-regulatório, as regras são simplesmente ditadas pelo código imperativamente. Em um contexto em que ferramentas tecnológicas não-normativas dominam o ambiente regulatório, parecemos estar sujeitos à regra da tecnologia e não ao Estado de Direito. A tecno-regulação sinaliza o desaparecimento de nossa capacidade de argumentar e resistir e, assim, pode resultar em um desvio ainda maior dos valores que nos tornam "humanos", ao pensarmos nas relações de poder e contestações; bem como na esfera da verdade e da justiça regida pelo Estado de Direito.

No entanto, não deve ser a intenção da lei governar este processo de forma a dificultar ou minar o avanço da tecnologia. Diferentemente, devemos estar conscientes de que se a tecno-regulação através do código está crescendo mais rapidamente do que a nossa capacidade de garantir os direitos fundamentais dos usuários como, por exemplo, segurança e privacidade, é necessário um enquadramento legal adequado para responder a esses novos desafios jurídicos. A reflexão profunda que devemos ter sobre isso engloba indagar também sobre a possibilidade de irmos além do tradicional "dever ser" dos sistemas legais para pensarmos no direito como uma técnica de regulação também capaz de regular através do design, de códigos e arquiteturas. [1047]

A ordem jurídica, diferentemente de outras ordens sociais, regulamenta o comportamento humano por meio de uma técnica específica. Uma vez que essa técnica regula outras técnicas que orientam os comportamentos e, além disso, os processos de inovação tecnológica, podemos, portanto, conceber a lei como uma meta-tecnologia.[1048]

[1047] Cracking down on autonomy: three challenges to design in IT Law. Ugo Pagallo. Ethics and Information Technology, vol. 14 (4), 2012.
[1048] On the legal implications of regulation by technology: of law and things. Ugo Pagallo (in press).

Para evitar um cenário de tecno-regulação (onde '*code is law*') que se sobreponha às regulamentações jurídicas vigentes, bem como ao norteamento ético que se pretende na esfera pública e na produção das Coisas, devemos buscar uma regulação mais efetiva destas tecnologias, a partir de uma perspectiva meta-tecnológica do Direito.[1049]

As maneiras diferentes em que podemos entender os propósitos normativos da lei como uma meta-tecnologia nos levam a expandir nossa visão jurídica tradicional. Por exemplo, uma abordagem meta-regulatória no campo da automação legal deve nos permitir determinar se, e até que ponto, os legisladores não devem (ou não podem) delegar decisões a sistemas automatizados. Além disso, o enfoque deve ser sobre o impacto da tecnologia no Estado de Direito, no próprio papel da lei e em como a tecnologia compete com outros sistemas regulatórios. Devemos também prestar atenção aos princípios e valores que estão em jogo ao delegarmos a tomada de decisões a sistemas automatizados, nomeadamente com questões de interpretação e deliberação. Por fim, a distinção entre decisões automáticas e não-automáticas da lei e sua legitimidade podem implicar no advento de novos problemas legais, por exemplo, novos *hard cases*. [1050]

Tendo em mente a importância da lei como uma ferramenta para regular comportamentos, bem como considerando que seus critérios também levam em conta a necessidade de garantir os direitos fundamentais, preservando simultaneamente a autonomia humana, o Estado de Direito (*Rule of Law*) deve orientar a tecnologia e não o oposto.

Portanto, diante dos crescentes riscos impostos pelo avanço da tecno-regulação, ampliados pela disseminação do ambiente de IoT, o *Rule of Law* deve ser visto como a premissa para o desenvolvimento tecnológico, ou como uma meta-tecnologia, que deve orientar a maneira como a tecnologia molda os comportamentos e não o contrário – o que muitas vezes resulta na violação de direitos humanos e fundamentais.

[1049] Disponível em: <https://plato.stanford.edu/entries/rule-of-law/>. Acesso em: 24 mai. 2017.
[1050] The Pros and Cons of Legal Automation, and its Governance. Ugo Pagallo, Massimo Durante. European Journal of Risk Regulation, vol. 7 (2), 2016.

Com relação ao papel do Direito, declara Paul Ohm:[1051]

> Se nos preocuparmos com toda a população sendo arrastada irreversivelmente à beira de danos, devemos regular de antemão, porque a esperança de regular após o fato é o mesmo que não regular de forma alguma. Desde que a nossa identidade seja separada da base de dados da ruína por um alto grau de entropia, podemos descansar tranquilamente. Mas, à medida que os dados são ligados a outros dados, e à medida que os adversários diminuem a entropia, cada um de nós logo será lançado à beira da ruína. [1052]

Para que o direito atue adequadamente como meta-tecnologia, deve estar lastreado por diretrizes éticas condizentes com a era da hiperconectidade. Nesse sentido, o avanço tecnológico deve ser guiado de maneira dentológica e novo-materialista, para que, ainda que com uma perspectiva centrada no ser-humano, consiga compreender a capacidade de influência dos agentes não-humanos, visando atingir uma melhor regulação, principalmente para as tecnologias mais autônomas, pensando na preservação dos direitos fundamentais dos indivíduos e na preservação da espécie humana.

Nesse sentido, conforme pontua Josh Lovejoy:[1053]

> Como profissionais centrados no ser humano, temos uma tremenda oportunidade de moldar um mundo mais humanista e inclusivo em conjunto com a IA, e começa por lembrar nossas raízes: encontrar e atender às necessidades humanas reais, defender os valores humanos e planejar o aumento, não a automação. . O papel da IA não deveria ser encontrar a agulha no palheiro para nós, mas mostrar quanto feno ela pode clarear para que possamos ver melhor a agulha nós mesmos.[10541055]

[1051] OHM, Paul. *Broken Promises of Privacy:* responding to the surprising failure of anonymization. *UCLA Law Review*, v. 57, p. 6, 2010.

[1052] Tradução livre do autor. No original: *If we worry about the entire population being dragged irreversibly to the brink of harm, we must regulate in advance because hoping to regulate after the fact is the same as not regulating at all. So long as our identity is separated from the database of ruin by a high degree of entropy, we can rest easy. But as data is connected to data, and as adversaries whittle down entropy, every one of us will soon be thrust to the brink of ruin.*

[1053] LOVEJOY, Josh. The UX of AI. *Using Google Clips to understand how a human-centered design process elevates artificial intelligence*. Disponível em: <https://design.google/library/ux-ai/. Acesso em: 24 mai. 2017.

[1054] Tradução livre do autor. No original: *As human-centered practitioners, we have a tremendous opportunity to shape a more humanist and inclusive world in concert with AI, and it starts by remembering our roots: finding and addressing real human needs, upholding human values, and designing for augmentation, not automation. The role of AI shouldn't be to find the needle in the haystack for us, but to show us how much hay it can clear so we can better see the needle ourselves.*

[1055] Disponível em: https://weforum.ent.box.com/v/AI4Good?platform=hootsuite>. Acesso em: 24 mai. 2017.

O Direito, lastreado por um embasamento ético adequado, servirá como um canalizador do processamento de dados e demais materialidades tecnológicas evitando uma tecno-regulação nociva à humanidade. Nesse novo papel, é importante que o Direito oriente a produção e desenvolvimento de Coisas (artefatos técnicos) de forma a serem sensíveis a valores, por exemplo, regulando privacidade, segurança e ética *by design*. Em metáfora explicitada por Luciano Floridi, o Direito como meta-tecnologia funcionaria como tubulações adequadas à era digital, por onde todo o conteúdo e ações passariam.[1056]

Segundo Peter Verbeek:[1057]

> Ao projetar tecnologias robóticas, considerações éticas devem ser observadas. Os robôs usam algoritmos para tomar decisões, que incorporam valores e estruturas éticas. Além disso, os robôs têm implicações éticas para as práticas em que são utilizados, como cuidados de saúde, educação e interações sociais. Para abordar essas dimensões éticas dos robôs, a ética deve ser parte do processo de *design*, baseando-se em abordagens como a *Value Sensitive Design.*[1058]

Conforme mencionamos no item anterior, os artefatos técnicos possuem moralidade intrínseca em função de serem caracterizados pelos elementos da: (i) função técnica (para que serve?) e; (ii) plano de uso (como deve ser usado?), projetados por seres humanos. O desenho do plano de uso estreita a relação entre os engenheiros e os usuários. No entanto, engenheiros não possuem o monopólio do desenvolvimento dos planos de uso, da descrição ou da produção de artefatos. Esse desenvolvimento deve ser orientado pelo Direito a partir de um amplo debate na esfera pública sobre as questões éticas e jurídicas envolvidas, encarando o poder de agência das Coisas.

Sobre a necessidade de construirmos artefatos sensíveis a valores, já existem alguns exemplos por iniciativa de determinadas empresas. A montadora japonesa Toyota criou em parceria com a empresa Hino um dispositivo que mede o teor alcoólico do hálito do motorista e pode bloquear a partida do automóvel

---

[1056] FLORIDI, Luciano. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality.* Oxford Press. 2016.

[1057] VERBEEK, Peter, Moralizing Technology: Understanding and Designing the Morality of Things, Chicago / London, *The University of Chicago Press*,. 2011.

[1058] Tradução livre do autor: *When designing robotic technologies, ethical considerations should be taken into account. Robots use algorithms to make decisions, which embody ethical values and frameworks. In addition, robots have ethical implications for the practices in which they are used, like health care, education, and social interactions. In order to address these ethical dimensions of robots, ethics needs to be part of the design process, building on approaches like the Value Sensitive Design approach.*

caso o limite tolerável seja ultrapassado.[1059] Isso significa que tal artefato possui segurança *by design*. Outros exemplos podem ser dados. Um drone que não consegue fotografar nem filmar janelas, casas e apartamentos é um drone sensível ao valor da privacidade e intimidade. A ferramenta de anonimização citada no capítulo segundo, TOR, é um *software* orientado pelo valor da privacidade e com o valor que defendemos nesse trabalho, o "direito ao não-rastreio" (*privacy by design*). Uma arma que só dispara com a leitura da biometria do dono é um artefato dotado de segurança *by design,* já desenvolvido por algumas empresas. Assim como um *Bot* doméstico que pede para a criança falar as expressões "por favor" e "obrigado" ao interagir com elas, é um *bot* responsável, criado por engenheiros conscientes da influência que o *bot* pode exercer no comportamento das crianças, imputando *ética by design*.

Apesar disso ensejar debates legítimos sobre paternalismo jurídico, ético e tecnológico, o recurso do Direito como meta-tecnologia e regulação *by design* se mostra cada vez mais necessário para evitar uma tecno-regulacao nociva e demais violações a direitos humanos a partir das novas tecnologias. Por isso, os parâmetros, para serem politica e juridicamente legítimos, devem ser fruto de um intenso debate na esfera pública, de modo a espelhar a vontade e autonomia da sociedade.

Além do debate dialógico sobre o paternalismo que deve ser travado, para que o Direito consiga fazer um norteamento adequado, a sociedade, o Estado e as empresas devem debater na esfera pública, avaliando também seguintes indagações: (i) a aceitação social de determinada tecnologia envolve algum tipo de cálculo de risco? (ii) quais os critérios de aceitabilidade do risco de determinada tecnologia? (iii) Vantagens da atividade superam as desvantagens? (iv) existem alternativas mais eficientes? (v) o risco é voluntariamente assumido? (vi) as vantagens e desvantagens são distribuídas de forma equitativa? (vii) vale a pena reduzir os riscos? Devem levar em consideração, ainda, o fato de que não há artefatos ou ações tecnológicas "absolutamente seguras" e que o investimento em segurança em tecnologia pode impossibilitar o próprio desenvolvimento tecnológico.

[1059] Disponível em: <http://g1.globo.com/Noticias/Carros/0,,MUL1286685-9658,00.html>. Acesso em: 24 mai. 2017.

Segundo Peter Verbeek, as decisões e reflexões que precisamos fazer são extremamente difíceis, uma vez que exigem que consideremos uma grande quantidade de variáveis e interações entre nós e a tecnologia, bem como entre diferentes formas de tecnologia. No entanto, isso deve ser feito. Para Verbeek as tecnologias que têm consequências públicas (que são muitas delas) devem envolver o público no processo de design. Pode-se perguntar se é de fato viável envolver um público em grande parte desinformado e não especializado para participar dessas decisões, ou como esse processo pode funcionar, para não mencionar a logística pura e simples de gerenciar esse processo. Embora pareça prudente ou "justo" consultar o público sobre decisões sobre design, do ponto de vista prático, já temos exemplos de como a deliberação e a própria democracia falharam em diversos casos.[1060]

No entanto, o fato de que muitas pessoas não conhecem ou entendem o que realmente pode ser bom para elas, coloca um desafio adicional ao Estado e demais atores para que capacitem as pessoas para o debate, dentro de uma ótica habermasiana. A sociedade precisa ter consciência crítica e mais informação sobre como as tecnologias desempenham um papel ativo na influência das suas decisões (singulares, como híbridos, ou mesmo dentro de sistemas sociotécnicos), impactando a forma como percebemos e atuamos no mundo. Temos a responsabilidade jurídica, ética e democrática de determinar como permitiremos a tecnologia a influenciar nossa agência.

Verbeek revela uma nova direção para a essa discussão sobre como devemos abordar a tecnologia em termos de moralidade. Uma vez que a autonomia dos robôs e mais Coisas é susceptível de crescer, a sua regulamentação ética terá cada vez mais de ser especificamente concebida para prevenir comportamentos nocivos.

O Direito deve nortear a responsabilidade dos engenheiros e demais atores envolvidos no processo de *design* de Coisas inteligentes, para que pensem nos valores que entrarão no *design* dos artefatos, na sua função e no seu manual de uso. O que escapa do *design* e do manual de uso não depende do controle e

[1060] VERBEEK, Peter, Moralizing Technology: Understanding and Designing the Morality of Things, Chicago / London, *The University of Chicago Press*,. 2011.

influência do engenheiro e pode ser imprevisível, fruto inclusive da interação com outros actantes e sistemas sociotécnicos.

Empresas privadas possuem um relevante papel na concretização dos direitos constitucionais na esfera pública conectada. Por exemplo, sem a obrigação legal de rever eventuais filtragens algorítmicas e remoção de conteúdo não-informados ou o tratamento e compartilhamento de dados pessoais fora do objeto de determinado serviço e sem a devida proteção da privacidade e segurança dos consumidores, essas práticas tenderão a aumentar com o advento da Internet da Coisas.

O desafio, portanto, é observar e analisar estas práticas e mensurar sua importância e riscos, buscando guiar a tecnologia através de uma regulação jurídica mais eficiente, para que seja preservada a autonomia, privacidade e segurança do usuário.

Considerando a importância do Direito como um sistema (ou ferramenta; tecnologia) eficaz para se regular ações e nortear comportamentos, e tendo em vista, ainda, que seus critérios levam em consideração a liberdade individual de escolha entre diferentes cursos de ação, preservando a autonomia humana, bem como a garantia dos direitos fundamentais, a tecnologia deve ser guiada pelo Estado de Direito e não o oposto.

Por isso o Direito, como meta-tecnologia, deve fomentar e regular artefatos técnicos sensíveis a valores. Um artefato técnico dotado de imprevisibilidade e poder de agência significativo, deve ser orientado por valores constitucionalmente garantidos (deliberados na esfera pública) para ser considerado um artefato responsável e alinhado com o Estado Democrático de Direito.

Ao tratar da importância da regulação pelo Direito no cenário tecnológico, o jurista italiano Stefano Rodotà, declara que[1061] se não considerarmos a Internet como um espaço "constitucional", rico de garantias adequadas, podem prevalecer apenas as razões da segurança e do controle, conforme corre o risco de acontecer neste período. E, de toda forma, prevaleceriam as lógicas de mercado, que já estão impondo regras, visto que já a maioria das atividades on-line são de tipo

[1061] RODOTÀ, Stefano. *Palestra no Rio de Janeiro*. 2003. Disponível em: <http://www.rio.rj.gov.br/dlstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf>. Acesso em: 24 mai. 2017.

comercial e que a Web é considerada como uma gigantesca mina de dados pessoais, graças aos quais nasceu uma sociedade da vigilância e da classificação.

A insistência sobre a necessidade de considerar estes problemas de um ponto de vista "constitucional" indica com clareza quais são as direções que o Direito deve tomar se quiser respostas adequadas à maneira pela qual as tecnologias estão dando nova forma às nossas sociedades.[1062]

Para otimizar o efeito positivo e minimizar os danos oriundos do efeito disruptivo da regulação tecnológica avançada, é crucial que se compreenda seus impactos e consequências, considerando os aspectos técnicos e peculiaridades das novas formas de comunicação e, também, de regulação.

[1062] Speech in Rio de Janeiro. Stefano Rodotà, 2003. Disponível em: <http://www.rio.rj.gov.br/dlstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf>. Acesso em: 24 mai. 2017.

4
Conclusão

"We see the ocean navigated and the solid land traversed by steam power, and intelligence communicated by eletricity. Truly this is almost a miraculous era. What is before us no one can say, what is upon us no one can hardly realize. The progress of age has almost out-stripped human belief; the future is known only to Omniscience.
(Daniel Webster, ***1903****)*

*"**Vladimir:** I love you with all my soul.*
***Estragon:** I love you from the bottom of my heart.*
***Vladimir:** Because you are just a machine you have no real feelings.*
***Estragon:** No, you are the machine.*
***Vladimir:** I think you are.*
***Estragon:** No! You are a Robot! I am a human being. Just like the one that created you.*
***Vladimir:** It would be better if there were fewer people on this planet*
***Estragon:** Let it send this world back into the abyss!"*
(Conversa ao vivo entre dois Google Home Bots, ***2017****)*

A Internet das Coisas se torna mais proeminente a cada dia. Desenvolvida no contexto de evolução das tecnologias digitais e sendo considerada por muitos como um novo paradigma (Web 3.0), esse contexto representa um momento inédito e interessante tanto para o Estado quanto para empresas e cidadãos.

Os setores público e privado já demonstram estar atentos aos benefícios da IoT, baseados no uso de tecnologias integradas e no processamento massivo de dados. As estimativas recaem na geração de soluções mais eficazes para problemas ligados à gestão pública, eficiência produtiva, entre outros. Já existem diversos exemplos de aplicações de IoT pelo país, e essas experiências tendem a aumentar.

A ideia de ter dispositivos inteligentes interconectados permitindo uma interação eficiente entre máquinas e humanos, auxiliando estes em suas tarefas diárias, pode parecer um cenário exclusivamente benéfico, dado sua utilidade.

No entanto, os dados oriundos desses diversos dispositivos interconectados, gerados espontânea e deliberadamente pelos usuários, podem oferecer riscos a direitos constitucionais dos usuários, como privacidade e segurança. Consideradas individualmente, as informações processadas pelos dispositivos e plataformas *online* podem parecer irrelevantes e até inofensivas, porém quando combinadas ou quando se trata de dados sensíveis, podem expôr os cidadãos a prejuízos sem que esses tenham ainda plena consciência sobre os riscos atrelados ao uso dessas novas tecnologias. Portanto, é fundamental que os consumidores também estejam atentos a isso e sejam ainda mais cuidadosos com seus dados em um ambiente de Internet das coisas.

Por outro lado, diante do contexto de constante e intenso armazenamento, tratamento, compartilhamento e monetização dos dados que trafegam *online*, cabe também ao poder público buscar uma regulação jurídica adequada à tutela suficiente da privacidade dos indivíduos na era da hiperconectividade.

Para que cheguemos a uma regulação jurídica democraticamente legítima é crucial debatermos as noções de privacidade e ética que deverão nortear os avanços tecnológicos, refletindo sobre o mundo em que queremos viver e em como nos enxergamos nesse mundo de dados e máquinas relacionado ao novo cenário de IoT.

Por isso, nos debruçamos no primeiro capítulo deste trabalho sobre o conceito de tecnologia e inovação, buscando o correto enquadramento das funcionalidades de IoT neste contexto. Em seguida, tratamos da origem e construção do termo IoT explicitando sua relação com as características próprias da Web 3.0 em contraposição às fases anteriores da Web. Analisamos, em seguida, o estado da arte da IoT no Brasil no tocante ao seu potencial econômico e social, alertando para os riscos existentes à privacidade e à segurança dos usuários que demandam uma resposta regulatória do Estado de Direito ao avanço tecnológico, com intuito de proteger os direitos fundamentais.

No segundo capítulo deste trabalho mapeamos as regulamentações vigentes aplicáveis no Brasil e as principais propostas legislativas no tocante à proteção da privacidade e dos dados pessoais, contrastando as propostas legislativas com a regulação europeia. Justificamos a comparação em virtude do maior alinhamento da regulação europeia com o ordenamento jurídico brasileiro, em comparação com o sistema norte-americano, e por ter servido de inspiração

para a criação dos marcos regulatórios nacionais de proteção da privacidade. Concluimos o capítulo propondo uma reformulação do conceito de privacidade, mais adequado à IoT, sugerindo também novas possibilidades tecnológicas de auto-gerenciamento dos dados pessoais como ferramentas complementares à regulação legislativa.

No entanto, sem uma reflexão ética que norteie adequadamente a regulação jurídica, inclusive com relação à tutela da privacidade e dos dados pessoais, essa corre o risco de ser inócua ou nociva à coletividade. Por isso discutimos, no capítulo terceiro deste trabalho, as vertentes e perspectivas éticas que devem nortear o avanço deste novo mundo de dados fortemente impactado pelas novas características da IoT e da Inteligência Artificial.

A intensificação da interação homem-máquina e de decisões algorítmicas no contexto de IoT exigem novas lentes ontológicas e epistemológicas capazes de compreender melhor a influência desses elementos na esfera pública conectada e seu impacto na situação ideal de fala, além da necessidade de uma eficaz governança de dados. Sustentamos no capítulo terceiro que Coisas são dotadas de poder de agência e têm interagido com seres humanos de forma cada vez mais autônoma e imprevísivel devido a técnicas de *machine learning,* entre outras.

Com a tecnologia passando de simples ferramenta a agente tomador de decisões, o direito deve se reconstuir como ferramenta no mundo tecno-regulado, incorporando esses actantes a partir de um viés meta (como uma meta-tecnologia), construindo as bases normativas para uma regulação ética das novas tecnologias através do design. Por isso devemos aprimorar e fomentar modelos de *design* de tecnologia centrados no ser humano (*human-centered design*) e sensíveis a valores, regulando, por exemplo, ética, segurança e privacidade *by design* (*value sensitive design*).

O direito deve estar atento ao seu papel nesse contexto para, de um lado, não obstaculizar demasiadamente o desenvolvimento econômico e tecnológico em andamento e, por outro lado, regular com eficácia as práticas tecnológicas, visando coibir abusos e protegendo os direitos constitucionais vigentes.

Conforme reflexões arejadas de Stefano Rodotà:[1063]

> Nesta difícil tarefa são grandes as responsabilidades dos juristas. Eles também, no mundo global, estão engajados na busca de uma identidade, apresentando-se ora como "mercadores do direito", ora como racionalizadores da ordem econômica, ora como políticos dos direitos fundamentais, como projetistas de um futuro que a mutabilidade do presente parece tornar inalcançável. Se quiserem vencer o desafio da globalização, devem ter a força intelectual de compreender que deles espera-se uma forte inovação dos instrumentos jurídicos, a capacidade de trabalhar sobre os princípios antes do que sobre os detalhes, a atenção para a universalidade num mundo que não pode perder as diversidades. E as lógicas do mundo global exigem que eles não sejam frios espectadores dos grandes processos em curso. Não se pode ser neutro quando é necessário não apenas fazer com que sobreviva, mas fortalecer a democracia e os direitos fundamentais.

Concluimos, portanto, sustentando que a maneira como nos relacionamos com máquinas e algoritmos tende a ser cada vez mais intensa. Neste contexto de Internet das coisas, a governança e a segurança dos dados serão fundamentais. Benefícios e riscos para empresas, Estado e cidadãos devem ser sopesados de forma cautelosa, em conjunto com uma visão deontológia e de garantia de direitos fundamentais e humanos.

[1063] RODOTÀ, Stefano. *Palestra.* Trad. Myriam de Filippis. Rio de Janeiro, 2003. p. 11. Disponível em: <www.rio.rj.gov.br/dlstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf>. Acesso em: 31 mar. 2017.

5

Referências bibliográficas

ABBATE, Janet. **Inventing the Internet**. Massachusetts: Massachusetts Institute of Technology, 1999.

ABITEBOUL, Serge; ANDRÉ, Benjamin; KAPLAN, Daniel. Managing your digital life. **Communications of the ACM**, v. 58, n. 5, p. 35, may. 2015.

ACCENTURE. **Digital Trust in the IoT Era**, 2015. Disponível em: <https://www.accenture.com/t20160318T035041__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-3-Digital-Trust-IoT-Era.pdf>. Acesso em: 31 jan. 2017.

_____. **From productivity to outcomes**: using the Internet of things to drive future business strategies, 2015. Disponível em <https://www.accenture.com/t20150527T211103__w__/fr-fr/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/fr-fr/PDF_5/Accenture-CEO-Briefing-2015-Productivity-Outcomes-Internet-Things.pdf>. Acesso em 28 jun. 2016.

ADVANCED MP. Environmental impact of IoT. **Advanced MP**, [s.d.]. Disponível em: <http://www.advancedmp.com/environmental-impact-of-iot/>. Acesso em: 31 jan. 2017.

AGAZZI, Evandro. El Impacto Epistemológico De La Tecnología. **Argumentos**, [s.d.]. Disponível em: <http://www.argumentos.us.es/numero1/agazzi.htm>. Acesso em: 31 mar. 2017.

AGHAEI, Sareh; NEMATBAKHSH, Mohammad Ali; FARSANI, Hadi Khosravi. Evolution of the World Wide Web: from web 1.0 to web 4.0. **Internet Journal of Web & Semantic Technology**, v. 3, n. 1, jan. 2012. Disponível em: <http://airccse.org/journal/ijwest/papers/3112ijwest01.pdf>. Acesso em: 27 mar. 2017.

ALLSEEN ALLIANCE MERGES with Open Connectivity Foundation to Accelerate the Internet of Things. **Allseen Alliance**, Beaverton, out. 2016. Disponível em: <https://allseenalliance.org/allseen-alliance-merges-open-connectivity-foundation-accelerate-Internet-things>. Acesso em: 25 jan. 2017

ALMEIDA, Kamila. Projeto pioneiro no Brasil, botão de pânico ajuda a reduzir violência no ES. **ZH Notícias**, abr. 2013. Disponível em: <http://zh.clicrbs.com.br/rs/noticias/noticia/2013/04/projeto-pioneiro-no-brasil-botao-de-panico-ajuda-a-reduzir-violencia-no-es-4119173.html>. Acesso em: 25 jan. 2017.

ALMEIDA, Virgilio A. F.; DONEDA, Danilo; MONTEIRO, Marília. Governance Challenges for the Internet of Things. **IEEE Internet Computing**, jul./ago. 2015.

AMARAL, Gustavo Rick. Uma dose de pragmatismo para as epistemologias contemporâneas: Latour e o parlamento das coisas. **Teccogs: Revista Digital de Tecnologias Cognitivas**, São Paulo, n. 12, p. 92-118, jul-dez. 2015.

ANDRADE, Thales de. Inovação tecnológica e meio ambiente: a construção de novos enfoques. **Ambiente & Sociedade**, v. VII, n. 1, p. 89-106, jan./jun. 2004.

ARADAU, Claudia et al. **Discourse/materiality.** Critical security methods: New frameworks for analysis, p. 57-84, 2014.

ARANTES, Esther Maria de Magalhães. Proteção Integral à Criança e ao Adolescente: Proteção *versus* Autonomia. **Psicologia Clínica**, n. 2, v. 21, p. 431-450, 2009.

ARNAUDO, Dan. Computational Propaganda in Brazil: Social Bots during Elections. **Computational Propaganda Research Project**, Working Paper n. 2017.8, 2017.

ASHRAF, Qazi Mamoon; HABAEBI, Mohamed Hadi. Autonomic schemes for threat mitigation in Internet of Things. **Journal of Network and Computer Applications**, v. 49, 2015.

ASHTON, Kevin. That 'Internet of Things' Thing. **RFID Journal**, 22 jun. 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986>. Acesso em: 29 mar. 2017.

ASSANGE, Julian et al. **Cypherpunks: Liberdade e o future da Internet**. São Paulo: Boitempo, 2013.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. **Computer networks**, v. 54, n. 15, 2010.

BARAD, Karen. **Meeting the universe halfway:** Quantum physics and the entanglement of matter and meaning. duke university Press, 2007.

BAGGIO, Bobbe; BELDARRAIN, Yoany. **Anonymity and Learning in Digitally Mediated Communications:** Authenticity and Trust in Cyber Education. IGI Global, 2011.

BAJARIN, Tim. The Next Big Thing for Tech: The Internet of Everything. **Time**, jan. 2014. Disponível em: <http://time.com/539/the-next-big-thing-for-tech-the-Internet-of-everything/>. Acesso em: 28 mar. 2017.

BANDYOPADHYAY, Debasis; SEN, Jaydip. Internet of things: Applications and challenges in technology and standardization. **Wireless Personal Communications**, v. 58, n. 1, 2011.

BANISAR, David. National Comprehensive Data Protection/Privacy Laws and Bills 2016. *ARTICLE 19:* **Global Campaign for Free Expression**, 2016. Disponível em: <https://ssrn.com/abstract=1951416>. Acesso em: 07 fev. 2017.

BAPTISTA, Rodrigo. Porque a Internet das Coisas implica em gerenciar contextos, e não dados. **Computerworld**, 02 jul. 2015. Disponível em: <http://www.tirio.org.br/info/36007/porque-a-Internet-das-coisas-implica-em-gerenciar-contextos-e-nao-dados>. Acesso em: 31 mar.

BARBOSA, Denis Borges. **Uma Introdução à Propriedade Industrial**. 2. ed. rev. e atual. Rio de Janeiro: Lumen Juris, 2003.

BARKER, Colin. 25 billion connected devices by 2020 to build the Internet of Things. **ZDNet**, 11 nov. 2014. Disponível em: <http://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-Internet-of-things/>. Acesso em: 27 mar. 2017.

BARRY, A. **Political Machines:** Governing a Technological Society. London: Athlone Press. 2001.

BASSI, Silvia. IBM transforma Internet das Coisas em investimento estratégico bilionário. **ComputerWorld**, ago. 2015. Disponível em:

<http://computerworld.com.br/ibm-transforma-Internet-das-coisas-em-investimento-estrategico-bilionario>. Acesso em: 28 abr. 2017.

BAUMAN, Zygmunt. Sobre a internet, anonimato e irresponsabilidade In: **Isto não é um diário.** Rio de Janeiro: Zahar, 2012.

BAURA, Gail. **Engineering Ethics:** An Industrial Perspective. Cambridge: Academic Press, 2006.

BELLI, Luca; SCHWARTZ, Molly; LOUZADA, Luiza. Selling your soul while negotiating the conditions: from notice and consent to data control by design**. Health Technology**, 2017, p. 8. Disponível em: <https://link.springer.com/article/10.1007/s12553-017-0185-3>. Acesso em: 28 set. 2017.

BENAKOUCHE, Tamara. Tecnologia é sociedade: contra a noção de impacto tecnológico. **Cadernos de pesquisa**, n. 17, p. 1-28, set. 1999.

BENKLER, Y. **The Wealth of Networks**: how social production transform markets and freedom. New Haven: Yale University Press, 2006.

BENTHAM, Jeremy. **Os pensadores**. São Paulo: Abril Cultural, 1979.

BERGEL, Salvador D. In: CORREA, Carlos M. (Coord.). **Derecho de Patentes, el nuevo regimen legal de las invenciones y los modelos de utilidad.** Buenos Aires: Ed. Ediciones Ciudad Argentina, 1996.

BESSIS, Nik e DOBRE, Ciprian. **Big Data and internet of things:** a roadmap for smart environments. Nova York: Springer International Publishing, 2014.

BIG THINK. Web 3.0. **Youtube**, abr. 2012. Disponível em: <https://www.youtube.com/watch?v=EMkTic4ztU8>. Acesso em: 27 mar. 2017.

BINDER, Denis. **The Increasing Application of Criminal Law to Disasters and Tragedies.** Natural Resources & Environment, v. 30, n. 3, 2016.

BIONI, Bruno Ricardo. A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. In: ROVER, Aires José; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo. **Direito e novas tecnologias**. Florianópolis: CONPEDI, 2014.

BINGHAM, Tom. **The Rule of Law**. Penguin, 2010.

BLOOR, David. **Knowledge and social imagery**. London: Routledge & Kegan Paul, 1976.

BOBBIO, Norberto. **Igualdade e liberdade**. Tradução: Carlos Nelson Coutinho. 2. ed. Rio de Janeiro: Ediouro, 1997

BOLTON, David. 100% of reported vulnerabilities in the Internet of Things are Avoidable. **Applause**, sep. 2016. Disponível em: <https://arc.applause.com/2016/09/12/Internet-of-things-security-privacy/>. Acesso em: 31 jan. 2017.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010.

_____. **Lei no** 9.279**, de 14 de maio de 1996**. Regula direitos e obrigações à propriedade industrial. Brasília: Diário Oficial da União (DOU). Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9279.htm>; . Acessado em 02 dez. 2017.

BREWSTER, Tom. **When machines take over**: our hyperconnected world. BBC, 25 jan. 2014. Disponível em: <http://www.bbc.com/capital/story/20140124-only-connect>. Acesso em: 27 mar. 2017.

BRILL, Mark. Are Smartwatches The New Sandwich Toaster? **Brands, Innovation and Creative Technologies**, 27 mar. 2015. Disponível em: <https://brandsandinnovation.com/2015/03/27/are-smartwatches-the-new-sandwich-toaster/>. Acesso em: 30 jan. 2017.

_____. The Internet of Useless Things and how to avoid it. **SlideShare**, jun. 2015. Disponível em: <http://pt.slideshare.net/MarkBrill/the-Internet-of-useless-things-and-how-to-avoid-it>. Acesso em: 31 jan. 2017.

BRISBOURNE, Alex. Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things? **Wired**, [201-]. Disponível em: <https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-Internet-things/>. Acesso em: 25 jan. 2017.

BUCHANAN, Robert Angus. History of technology. **Encyclopædia Britannica**, 27 fev. 2017. Disponível em: <https://global.britannica.com/technology/history-of-technology/The-Industrial-Revolution-1750-1900>. Acesso em: 02 mai. 2017.

BURRUS, Daniel. The Internet of Things Is Far Bigger Than Anyone Realizes. **Wired**, [s.d.]. Disponível em: <http://www.wired.com/2014/11/the-Internet-of-things-bigger/>. Acesso em: 29 mar. 2017.

BYRNE, Michael. The Internet of Cows Is Real. **Motherboard**, abr. 2016. Disponível em: <http://motherboard.vice.com/read/the-Internet-of-cows-Internet-of-things-agriculture>. Acesso em: 25 jan. 2017.

CALHOUN, Craig (ed.). **Habermas and the Public Sphere**. The MIT Press, 1992

CALLON, Michel. Society in the making: the study of technology as a tool for sociological analysis. In: BIJKER, Wiebe E.; HUGHES, Thomas P; PINCH, Trevor F. (Eds.). **The social construction of technological systems**: new directions in the sociology and history of technology. Cambridge (MA): The MIT Press, 1989.

CANOTILHO, José Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra. Almedina. 1998.

CAPANEMA, Walter Aranha. **O direito ao anonimato:** uma nova interpretação do art. 5o, IV, CF. Disponível em: <http://www.avozdocidadao.com.br/images_02/artigo_walter_capanema_o_direito_ao_anonimato.pdf>. Acesso em: 28 nov. 2017.

CARDOSO, Carlos. A Internet das Coisas Inúteis: EggMinder. **Meio Bit**, nov. 2013. Disponível em: <http://meiobit.com/271383/thinkgeek-egg-minder-smart-bandeja-pra-ovo/>. Acesso em: 31 jan. 2017.

CASTELLS, M. **A Sociedade em Rede** – A Era da Informação: Economia, Sociedade e Cultura. Vol. I. São Paulo: Paz e Terra, 1999.

_____. **A sociedade em rede**. Volume I. 8. ed. rev. e ampl. Tradução de Roneide Venancio Majer. São Paulo: Paz e Terra, 2005.

CASTRO, Marco Aurélio. *Personalidade jurídica do robô e sua efetividade*. Salvador: 2009.

CAVALCANTI, Jose Carlos. The new ABC of ICTs (Analytics + Big Data + Cloud Computing): a complex trade off between IT and CT costs. In: MARTINS, Jorge Tiago; MOLNAR, Andreea (Orgs.). **Handbook of Research on Innovation in Information Retrieval, analysis and management**. Hershey: IGI Global, 2016.

CAVALLI, Olga. Internet das Coisas e Inovação na América Latina. 2016 (mimeo).

CAVOUKIAN, Ann. **Privacy by Design**: The Seven Foundational Principles. **Information and Privacy Commissioner of Ontario**, Toronto, jan. 2011. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 31 mar. 2017.

CENTRO DE ESTUDOS, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet**, [201-?]. Disponível em: <http://cartilha.cert.br/ransomware/>. Acesso em: 30 mar. 2017.

CERKA, Paulius et al. Liability for damages caused by artificial intelligence. **Computer Law & Security Review**, vol. 31, n. 3, jun. 2015.

CERUZZI, Paul E. The Internet before Commercialization. In: _____; ASPRAY, William (eds.). **The Internet and American Business**. Cambridge (MA): The MIT Press, 2008, p. 9-43.

CHABRIDON, Sophie et al. A survey on addressing privacy together with quality of context for context management in the internet of things. **Annals of telecommunications-annales des télécommunications,** v. 69, n. 1-2, 2014.

CHAVES, Luis Fernando Prado; GOMES, Maria Cecilia Oliveira. Por que a Internet das Coisas revolucionará o Direito Digital? **Justificando,** 20 fev. 2017. Disponível em: <http://justificando.cartacapital.com.br/2017/02/20/por-que-Internet-das-coisas-revolucionara-o-direito-digital/>. Acesso em: 21 fev. 2017.

CISCO. The Zettabyte Era: Trends and Analysis. **Cisco**, jun. 2016. Disponível em <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html>. Acesso em: 27 mar. 2017.

COBB, Stephen. 10 Things to know about the October 21 DDoS Attacks. **We live security**, 24 out. 2016. Disponível em: <http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/>. Acesso em: 31 jan. 2014.

Code Is Law: On Liberty in Cyberspace. Lawrence Lessig. **Harvard Magazine**. Disponível em: <http://harvardmagazine.com/2000/01/code-is-law-html – Accessed 24/05/2017>. Acesso em: 24 mai. 2017.

COLE, George S. Tort Liability For Artificial Intelligence And Expert Systems. **Computer/Law Journal**, vol. 10, n. 2, 1990.

CONCEITO de tecnologia. **Conceito.de**, ago. 2015. Disponível em: <http://conceito.de/tecnologia#ixzz4YfibhpPs>. Acesso em: 27 mar. 2017.

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. **Serviços e Competitividade Industrial no Brasil**. Brasília: CNI, 2014. Disponível em:

<http://arquivos.portaldaindustria.com.br/app/conteudo_24/2014/12/09/517/ServioseCompetitividadeIndustrialnoBrasil.pdf>. Acesso em: 28 mar. 2017.

CONSUMER TECHNOLOGY ASSOCIATION. **Internet of Things**: a Framework for the Next Administration (White Paper), 2016. Disponível em: <http://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf>. Acesso em: 31 jan. 2017.

CORMODE, Graham; KRISHNAMURTHY, Balachander. Key diferences between Web 1.0 and Web 2.0. **First Monday**, v. 12, n. 6, jun. 2008. Disponível em: <http://firstmonday.org/ojs/index.php/fm/article/view/2125/1972>. Acesso em: 27 mar. 2017.

CORRÊA, Alexandra Barbosa De Godoy. Patentes de Medicamentos e o Princípio da Função Social da Propriedade no Brasil. **Revista Propiedad Intelectual**, Mérida, Venezuela, ano XIII, n. 17, p. 59-82, jan./dez. 2014.

COSTA, C. Razões para o utilitarismo. **Ethic@.** Florianópolis: UFSC, v.1, n. 2, p. 155-174, 2002.

CROUAN, Raph. Corporates must help stop us creating an Internet of Useless Things. **NewStatesman**, jun. 2016. Disponível em: <http://tech.newstatesman.com/iot/Internet-useless-things>. Acesso em: 31 jan. 2017.

DAHIR, Hazim, DRY, Bil e PIGNATARO Carlos. **People, Processes, Services, and Things:** Using Services Innovation to Enable the Internet of Everything. Nova York: Business Expert Press, 2015.

DARMOUR, Jennifer. The Internet of You: When Wearable Tech and the Internet of Things Collide. **Artefact Group**, [s.d.]. Disponível em: <https://www.artefactgroup.com/articles/the-Internet-of-you-when-wearable-tech-and-the-Internet-of-things-collide/>. Acesso em: 29 mar. 2017.

DATA IS GIVING rise to a new economy. **Economist,** 6 may. 2017. Disponível em: <https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>. Acesso em: 03 jul. 2017.

DENHAM, Elizabeth. Promoting privacy with innovation within the law (Speech). In: **30TH ANNUAL CONFERENCE OF PRIVACY LAWS AND BUSINESS**, Cambridge, 4 jul. 2017. Disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/promoting-privacy-with-innovation-within-the-law/>. Acesso em: 05 jul. 2017.

DHANJANI, Nitesh. **Abusing the Internet of Things:** Blackouts, Freakouts, and Stakeouts. Newton: O'Reilly Media, Inc., 2015.

DIAKOPOULOS, Nicholas. Algorithm Accountability – Journalistic investigation of computational power structures. **Digital Journalism**, v. 3, n. 3, p. 398, 2015

DN. Tay, a inteligência artificial racista e cheia de ódio da Microsoft, voltou a aparecer. **DN**, mar. 2016. Disponível em: <>. Acesso em: 16 ago. 2017.

DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul De. (Eds.) **Reloading Data Protection:** Multidisciplinary Insights and Contemporary Challenges. London: Springer, 2014

DONEDA, Danilo, ALMEIDA, Virgilio; MONTEIRO, Marilia. Governance challenges for the Internet of Things. **IEE Computer Society**, v. 19, n. 4, p. 56-59, 2015.

DONEDA, Danilo,. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DORADOR, Marcelo. Inauguração do Centro Integrado de Monitoramento em SBC. **ABC do ACB**, 02 abr. 2014. Disponível em:< http://www.abcdoabc.com.br/sao-bernardo/noticia/inauguracao-centro-integrado-monitoramento-sbc-18735>. Acesso em: 11 abr. 2017.

DREHER, Felipe. IoT pode agregar US$ 352 bilhões à economia brasileira até 2022. **Computer World**, jun. 2015. Disponível em: <http://computerworld.com.br/iot-pode-agregar-us-352-bilhoes-economia-brasileira-ate-2022>. Acesso em: 25 jan. 2017.

DUHIGG, Charles. How companies know your secrets. **The New York Times**, fev. 2012. Disponível em: <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp>. Acesso em: 25 set. 2017.

DUTTA, Soumitra; LANVIN, Bruno; VINCENT-WUNSCH, Sacha (Eds.). **The Global Innovation Index 2016**: Winning with Global Innovation. Cornell University, INSEAD and WIPO: Ithaca, Fontainebleau and Geneva, 2016.

EINSTEIN, Ben. The Internet of (Dumb) Things. **Bolt**, feb. 2014. Disponível em: <https://blog.bolt.io/the-Internet-of-dumb-things-49d102018e16#.9ljsxiy4m>. Acesso em: 31 jan. 2017.

EM 2016 advogados recorreram a tecnologia para espantar a crise. **Terra Notícias**, 3 jan. 2017. Disponível em:http://olhardigital.uol.com.br/lu-explica/noticia/veja-como-a-tecnologia-pode-deixar-a-sua-casa-mais-segura/64971 <https://noticias.terra.com.br/dino/em-2016-advogados-recorreram-a-tecnologia-para-espantar-a-crise,2cbd6a01657d0cf1c6c60003480d6bf31euayidm.html>. Acesso em: 27 mar. 2017.https://noticias.terra.com.br/dino/em-2016-advogados-recorreram-a-tecnologia-para-espantar-a-crise,2cbd6a01657d0cf1c6c60003480d6bf31euayidm.html

ESTRADA, Manuel Martín Pino. O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade. **Revista de Direito do Trabalh***o*, v. 172, p. 43, nov./dez. 2016.

EU Data Protection Regulation. Data Protection by Design and by Default. **EU Data Protection Regulation**, [s.d.] Disponível em: <http://www.eudataprotectionregulation.com/data-protection-design-by-default>. Acesso em: 31 mar. 2017.

EUROPEAN DATA PROTECTION SUPERVISOR. **Towards a new digital ethics:** data, dignity and technology, 2015, p. 6. Disponível em: <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf>. Acesso em: 16 fev. 2017.

FARIA, Cristiano Ferri Soares de. **O Parlamento aberto na era da Internet**: pode o povo colaborar com o legislativo na elaboração das leis? Brasília: Ed Câmara, 2012.

FEDERAL TRADE COMISSION. Internet of things: Privacy & Security in a Connected World. **FTC Staff Report**, 2015.

FEENBERG, Andrew. **Tecnologia, Modernidade e Democracia**. Org. e trad.: Eduardo Beira. Lisboa: MIT Portugal/ IN^{+}/ Inovatec, 2015.

FERNÁNDEZ, Maria. **Posthumanism,** New Materialism and Feminist Media Art.

FERREIRA, Rubens da Silva. Ciência e Tecnologia no Olhar de Bruno Latour. **Inf. Inf.**, Londrina, v. 18, n. 3, p. 275-281, set./dez. 2013.FISHER, Dennis. FTC Warns of Security and Privacy Risks in IoT Devices. **On The Wire**, 3 jun. 2016. Disponível em: <https://www.onthewire.io/ftc-warns-of-security-and-privacy-risks-in-iot-devices/>. Acesso em: 31 jan. 2017.

_____. The Internet of Dumb Things. Digital Guardian, 13 out. 2016. Disponível em: <https://digitalguardian.com/blog/Internet-dumb-things>. Acesso em: 01 fev. 2017.

FILHO, Sérgio Cavalieri. O direito do consumidor no limiar século XXI. Revista de Direito do Consumidor. Revista dos Tribunais, nº 35, jul/set. 2000, p. 105.

FISCHER-HÜBNER, Simone; WRIGHT, Matthew (Ed.). Privacy Enhancing Technologies: 12th International Symposium, PETS 2012, Vigo, Spain, July 11-13, 2012, **Proceedings.** Nova York: Springer, 2012.

FLORIDI, Luciano. **The Fourth Revolution: How the Infosphere is Reshaping Human Reality.** Oxford Press. 2016.

FOLLETT, Jonathan. **Designing for Emerging Technologies:** UX for Genomics, Robotics, and the Internet of Things. Newton: O'Reilly Media, Inc., 2014.

FOX, Nick. **New materialist social inquiry:** designs, methods and the research-assemblage. 2014. Disponível em: <http://www.tandfonline.com/doi/full/10.1080/13645579.2014.921458>. Acesso em: 19 set. 2017.

FOX, Nick J.; ALLDRED, Pam. New materialista social inquiry: designs, methods and the research-assemblage. **International Journal of Social Research Methodology**, v. 18, n. 4, p. 399-414, 2015.

FORTES, Vinicius Borges. **Os direitos de privacidade e a proteção de dados pessoais na Internet.** Rio de Janeiro: Lumen Juris, 2016.

FISHER, Dennis. The Internet of dumb things. **Digital Guardian**, 13 out. 2016b. Disponível em: <https://digitalguardian.com/blog/Internet-dumb-things>. Acesso em: 1 fev. 2017.

_____. FTC warns of security and privacy risks in IoT devices. **On The Wire**, 3 jun. 2016a. Disponível em: <www.onthewire.io/ftc-warns-of-security-and-privacy-risks-in-iot-devices/>. Acesso em: 31 jan. 2017.

FRANKENA, Willian K. **Etica.** Rio de Janeiro : Zahar, 1969.

FREDETTE, John et al. The Promise and Peril of Hyperconnectivity for Organizations and Societies. In: INSEAD & World Economic Forum. **The Global Information Technology Report 2012**: Living in a Hyperconnected World. Genebra, 2012. p. 113-119. Disponível em: <https://pdfs.semanticscholar.org/68bb/365887b24ba1e541e3e2b8feb4569b94903d.pdf#page=139>. Acesso em: 27 mar. 2017.

FROOMKIN, Michael. Legal Issues in Anonymity and Pseudonymity, **The Information Society: An International Journal,** 1999.

FTC Staff Report. **Internet of Things**: privacy & security in a connected world. 2015. 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: 28 mar. 2017.

FUNG, A. **Deepening Democracy**: institutional innovations in empowered participatory governance. London: Verso Press, 2013.

GAGLIO, Salvatore; RE, Giuseppe Lo. **Advances onto the Internet of Things**. Nova York: Springer, 2014.

G1. De longe, hackers 'invadem' e controlam carro com jornalista dentro. **G1**, São Paulo, 22 jul. 2017. Disponível em: <http://g1.globo.com/carros/noticia/2015/07/de-longe-hackers-invadem-e-controlam-carro-com-jornalista-dentro.html>. Acesso em 30 mar. 2017.

G. Marx, **"What's in a Name?** Some Reflections on the Sociology of Anonymity", The Information Society 15(2):99-112 · May 1999.

GALIMBERTI, Umberto. **The human being in the age of technique Unisinos**. 2015.

GAMA CERQUEIRA, João da. **Tratado de Propriedade Industrial**. v. I, 2. ed. São Paulo: Ed. RT, 1982.

GETTING, Brian. Basic Definitions: Web 1.0, Web. 2.0, Web 3.0. **Pratical E-commerce**, abr. 2007. Disponível em: <http://www.practicalecommerce.com/articles/464-Basic-Definitions-Web-1-0-Web-2-0-Web-3-0>. Acesso em: 27 mar. 2017.

GIELFI, Marcella. "Internet das coisas" x "Internet de tudo": como isso vai mudar seu cotidiano em breve. **Ideia de Marketing**, 22 abr. 2013. Disponível em: <http://www.ideiademarketing.com.br/2013/04/22/Internet-das-coisas-x-Internet-de-tudo-como-isso-vai-mudar-seu-cotidiano-em-breve/>. Acesso em: 08 mai. 2017.

GILCHRIST, Alasdair. Introducing Industry 4.0. In: **Industry 4.0.** Nova York: Apress, 2016.

GILLESPIE, Tarleton. The Relevance of Algorithms. In: _____; BOCZKOWSKI, Pablo J.; FOOT, Kirsten A. (Eds.). Media Technologies: Essays on Communication, Materiality, and Society. **Cambridge (MA)***:* The MIT Press, 2014

GIURGIU, Luminita; BÂRSAN, Ghita. The prosumer – core and consequence of the web 2.0 Era. **Revista de Informatica Sociala**, ano V, n. 9, p. 53-59, jun. 2008.

GOVERNO ADIA, mais uma vez, megapiloto de Internet das Coisas no país. **TI RIO**, jun. 2015. Disponível em: <http://www.tirio.org.br/info/35868/governo-adia-mais-uma-vez-megapiloto-de-Internet-das-coisas-no-pais>. Acesso em 25 jan. 2017.

GRASSEGGER, Hannes & KROGERUS, Mikael. The Data That Turned the World Upside Down. **Motherboard**, 28 jan. 2017. Disponível em: <https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win>. Acesso em: 27 mar. 2017.

GREENGARD, Samuel. **The Internet of Things**. Cambridge (MA): The MIT Press, 2015.

GREENWALD, Glenn. **Sem lugar para se esconder**. Rio de Janeiro: Sextante, 2014.

GUO, Bin et al. From the internet of things to embedded intelligence. **World Wide Web**, v. 16, n. 4 2013

HABERMAS, Jürgen. Between **Facts and Norms:** Contributions to a Discourse Theory of Law and Democracy, Cambridge, Polity Press, 1992.

_____. **The Theory of Communicative Action**. Beacon Press. 1987. v. II

HAFNER, Katie; LYON, Matthew. **Where wizards stay up late**: the origins of the Internet. New York: Touchstone Edition, 1998.

HALLEVY, Gabriel. The Criminal Liability of Artificial Intelligence Entities: From Science Fiction to Legal Social Control. **Akron Intellectual Property Journal,** vol. 4, 2010.

HAPGOOD Fred. 20 Years of IT History: Connecting Devices, Data and People. **CIO**, 28 set. 2007. Disponível em: <http://www.cio.com/article/2438016/infrastructure/20-years-of-it-history--connecting-devices--data-and-people.html>. Acesso em: 29 mar. 2017.

HARAWAY, Donna. A cyborg manifesto: Science, technology and socialist-feminism in the late twentieth century. In: _____. **Simians, Cyborgs, and Women.** The Reinvention of Nature. Nova York: Routledge, 1991.

HARDY, Quentin. Working the Land and the Data. **The New York Times**, New York, nov. 2014. Disponível em: <https://www.nytimes.com/2014/12/01/business/working-the-land-and-the-data.html#>. Acesso em: 25 jan. 2017.

HARTMANN, I. **A auto regulação pelo código**: características, impacto e limites de um novo modelo. Rio de Janeiro: Malheiros (in press), 2015.

HEER, Tobias et al. Security Challenges in the IP-based Internet of Things. **Wireless Personal Communications,** v. 61, n. 3, p. 527-542, 2011.

HERNANDEZ, Leandro. Desafio da 'Internet das coisas' é impedir quebra de privacidade. **Notícias Uol,** 2015. Disponível em: <https://noticias.uol.com.br/opiniao/coluna/2015/07/18/desafio-da-Internet-das-coisas-e-impedir-quebra-de-privacidade.htm>. Acesso em: 21 fev. 2017.

HERSENT, Olivier; BOSWARTHICK, David; ELLOUMI, Omar. **The internet of things:** Key applications and protocols. Hoboken: John Wiley & Sons, 2011.

HEWLETT-PACKARD COMPANY. **Internet of Things Research Study Report**, jul. 2014. Disponível em: <http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VZRsHflVhHw>. Acesso em: 08 fev. 2017.

HOEPMAN, Jaap-Henk. Privacy Design Strategies. In: CUPPENS-BOULAHIA, Nora et al. (Eds.). **ICT Systems Security and Privacy Protection**. New York: London, 2014.

HOLLER, Jan et al. **From Machine-to-machine to the Internet of Things:** Introduction to a New Age of Intelligence. Cambridge: Academic Press, 2014.

HORN, Luiz Fernando Del Rio; LIMBERGER, Têmis. O diálogo entre o Marco Civil da Internet e o Código de PRoteção e Defesa do Consumidor: uma convivência legislativa em prol de um elevado nível de proteção aos dados. In: CONPEDI/UFPB. Direito do consumidor I [Recurso eletrônico on-line]. Coordenadores: Fernando

Antônio de Vasconcelos, Viviane Coêlho de Séllos Knoerr, Fernando Rodrigues Martins. Florianópolis : **CONPEDI**, 2014, p. 147.

HOWARD, Philip. **Pax Techinica**. New Haven: Yale University Press, 2015.

HOWER, Mike. As "Internet of Things" Grows, so do E-waste concerns. **Sustainable Brands**, 29 dez. 2014. Disponível em: <http://www.sustainablebrands.com/news_and_views/waste_not/mike_hower/Internet_things%E2%80%99_grows_so_do_e-waste_concerns>. Acesso em: 31 jan. 2017.

INTERNET OF caring things. **Trend Watching**, apr. 2014. Disponível em: <http://trendwatching.com/trends/Internet-of-caring-things/>. Acesso em: 31 jan. 2017.

INVISIBLE COMMITTEE. **Fuck off Google**, 2014. Disponível em: <https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2530/original/fuckoffgoogleeng.pdf>. Acesso em: 31 mar. 2017.

INTRONA, Lucas D. Algorithms, Governance, and Governmentality*:* On Governing Academic Writing. **Science, Technology***, & Human Values*, v. 41, n. 1, p. 17-49, 2016.

IT FORUM (Redação). Huawei e PUCRS abrem centro de inovação com foco em cidades inteligentes e IoT. **IT Forum**, abr. 2016. Disponível em: <http://itforum365.com.br/noticias/detalhe/119237/huawei-e-pucrs-abrem-centro-de-inovacao-com-foco-em-cidades-inteligentes-e-iot>. Acesso em: 25 jan. 2017.

JACOBY, David. Pesquisa: Como hackeei minha casa. **Kaspersky Lab**, 22 ago. 2014. Disponível em: <https://blog.kaspersky.com.br/pesquisa-como-hackear-minha-casa/3804/> Acesso em: 30 mar. 2017.

JING, Qi et. al. Security of the Internet of Things: perspectives and challenges**. Wireless Networks,** v. 20, n. 8, 2014.

JONAS, Hans. **O princípio da responsabilidade: ensaio de uma ética para a civilização tecnológica.** Ed. Contraponto. Rio de Janeiro. 2015.

JUDGE, Jenny. Are we liberated by tech – or does it enslave us? **The Guardian**, 9 dez. 2015. Disponível em: <https://www.theguardian.com/technology/2015/dec/09/are-we-liberated-by-tech-or-does-it-enslave-us>. Acesso em: 26 jan. 2017.

KANT, Immanuel. **Fundamentação da Metafísica dos Costumes** (Grundlegung zur Metaphysik der Sitten, 1785). Trad: Paulo Quintela: Edições 70, 2008.

_____. **A Paz Perpétua e Outros Opúsculos**, Lisboa, Edições 70, 1784 (1992)

KARASINSKI, Lucas. O que é tecnologia? **Tecmundo**, 29 jul. 2013. Disponível em: <https://www.tecmundo.com.br/tecnologia/42523-o-que-e-tecnologia-.htm>. Acesso em: 27 mar. 2017.

KELLMEREIT, Daniel e OBODOVSKI, Daniel. **The Silent Intelligence:** the internet of things. São Francisco: DnD Ventures, 2013.

KLINE, R. Construing "Technology" as "Applied Science": Public Rhetoric of Scientists and Engineers in the United States, 1880-1945. **Isis**, v. 86, n. 2, p. 194-221, jun. 1995. Disponível em: <http://www.jstor.org/stable/pdf/236322.pdf>. Acesso em: 28 mar. 2017.

KLITOU, Demetrius. **Privacy-Invading Technologies and Privacy by Design:** Safeguarding Privacy, Liberty and Security in the 21st Century. Berlin: Asser Press/Springer, 2014.

KNIGHT, Will. **"Forget Killer Robots...",** MIT Technology Review, Disponível em: <https://www.technologyreview.com/s/608986/forget-killer-robotsbias-is-the-real-ai-danger/>. Acesso em: 28 nov. 2017.

KOBIE, Nicole. The Useless Side of The Internet of Things. **Motherboard**, 5 fev. 2015. Disponível em: <http://motherboard.vice.com/read/the-useless-side-of-the-Internet-of-things>. Acesso em: 29 mar. 2017.

KROES, Peter. et al. **A Philosophy of Technology** From Technical Artefacts to Sociotechnical [s.l.]: Systems. Morgan & Claypool Publishers, 2011.

KYAS, Othmar. **How To Smart Home:** A Step by Step Guide to Your Personal Internet of Things. Wyk auf Föhr (Alemanha): Key Concept Press, 2015.

LANDIM, Wikerson. Wearables: será que esta moda pega? **Tec Mundo**, jan. 2014. Disponível em: <https://www.tecmundo.com.br/tecnologia/49699-wearables-sera-que-esta-moda-pega-.htm>. Acesso em: 31 jan. 2017.

LANE, Julia (org.). **Privacy, Big Data and the Public Good**: frameworks for engagement. Cambridge University Press. 2014.

LATOUR, Bruno. **A Esperança de Pandora**: Ensaios sobre a realidade dos estudos científicos. Trad.: Gilson Cesar Cardoso de Sousa. São Paulo: EDUSC, 2001.

_____. **Ciência em ação**: como seguir cientistas e engenheiros sociedade afora. Tradução de Ivone C. Benedetti. São Paulo: Editora UNESP, 2000.

_____. **Jamais Fomos Modernos**: Ensaio de Antropologia Simétrica. Trad.: Carlos Ireneu da Costa. Rio de Janeiro: Editora 34, 1994.

_____. On Technical Meditation – Philosophy, Sociology, Genealogy. **Common Knowledge**, v. 3, n. 2, p. 29-64, 1994.

_____; WOOLGAR, Steve. **Laboratory Life**: The Construction of Scientific Facts. Princeton: Princeton University Press, 1986.

LAW, John. and SINGLETON, V. **Performing technologies' stories:** on social construtivism, performance, and performativity. Technology and Culture. 2000.

LAW, John; LODGE, Peter. **Science for Social Scientists**. London: Macmillan Press, 1984.

LEINER, Barry M. et al. Brief History of the Internet. **Internet Society**, [199-?]. Disponível em: <http://www.Internetsociety.org/Internet/what-Internet/history-Internet/brief-history-Internet>. Acesso em: 29 mar. 2017.

LEITÃO, Thais. Sistema de identificação automática de veículos entrará em funcionamento em janeiro. **EBC**, out. 2012. Disponível em: <http://www.ebc.com.br/2012/10/sistema-de-identificacao-automatica-de-veiculos-entrara-em-funcionamento-em-janeiro>. Acesso em: 04 mai. 2017.

LEMKE, Thomas. **New Materialisms:** Foucault and the 'Government of Things'. Theory Culture & Society, april 2014.

LEMOS, André. [2] **A comunicação das coisas:** teoria ator-rede e cibercultura]. São Paulo: Annablume, 2013.

LEMOS, Ronaldo, et al. **O Direito da Internet das Coisas: desafios e perspectivas de IoT no Brasil.** 2018. Disponível em: <https://www.jota.info/artigos/o-direito-da-

internet-das-coisas-desafios-e-perspectivas-de-iot-no-brasil-09012018>. Acesso em: 27 mar. 2017.

LEMOS, Ronaldo e AFFONSO, Carlos. **Marco Civil da Internet Construção e Aplicação**. p. 30.

LERMAN, N. The Uses of Useful Knowledge: Science, Technology, and Social Boundaries in an Industrializing City. **Osiris**, v. 12, p. 39-59, 1997. Disponível em; <https://www.jstor.org/stable/pdf/301898.pdf>. Acesso em: 05 jan. 2017.

LESSIG, L. **Code and other laws of cyberspace**. New York: Basic Books, 1999.

LI, Shancang; XU, Li. **Securing the Internet of Things**. Cambridge: Syngress, 2017.

LIDDELL and SCOTT. **Greek-english Lexicon.** 7. ed. Nova Iorque: Oxford, 2001.

LIFEBOAT FOUNDATION. Web 3.0: The Third Generation Web is Coming. Special Report. **Lifeboat foundation – safeguarding humanity**, [20--]. Disponível em: <http://lifeboat.com/ex/web.3.0>. Acesso em: 28 mar. 2017.

LIMA, Leonardo. RFID e Privacidade? Experiências derrubam alguns mitos. **Cabtec GTI**, jul. 2014. Disponível em: <http://www.gradeti.com.br/blog/rfid/2014/07/rfid-e-privacidade-experiencias-derrubam-alguns-mitos/>. Acesso em: 29 mar. 2017.

LOHR, Steve. The Internet of Things and the Future of Farming. **Bits**, ago. 2015. Disponível em: <http://bits.blogs.nytimes.com/2015/08/03/the-Internet-of-things-and-the-future-of-farming/?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=3>. Acesso em: 25 jan. 2017.

LOUCHEZ, Alain; THOMAS, Valerie. E-waste and the Internet of Things. **ITU News**, 2014. Disponível em: <http://itunews.itu.int/en/4850-E-waste-and-the-Internet-of-Things.note.aspx>. Acesso em: 31 jan. 2017.

LOURENÇO, Daniel Braga. Direito dos animais: fundamentação e novas perspectivas. Porto Alegre: Sergio Antonio Fabris. Ed., 2008.

LOVEJOY, Josh. The UX of AI. **Using Google Clips to understand how a human-centered design process elevates artificial intelligence**. Disponível em: <https://design.google/library/ux-ai/. Acesso em: 24 mai. 2017.

LOVELACE JR., Berkeley e VIELMA, Antonio José. Friday's third cyberattack on Dyn 'has been resolved', company says. **CNBC**, 21 out. 2016. Disponível em: <http://www.cnbc.com/2016/10/21/major-websites-across-east-coast-knocked-out-in-apparent-ddos-attack.html> Acesso em: 08 fev. 2017.

MACEDO, Maria Fernanda Gonçalves; BARBOSA, A. L. Figueira. **Patentes, Pesquisa & Desenvolvimento**: um manual de propriedade industrial. Rio de Janeiro: Fiocruz, 2000.

MCEWEN, Adrian; CASSIMALLY, Hakim. **Designing the internet of things.** Hoboken: John Wiley & Sons, 2013.

MACEDO JÚNIOR, Ronaldo Porto. Privacidade, Mercado e Informação. **Justitia**, São Paulo, n. 61, p. 245-259, jan./dez. 1999.

MACHIN, Nathan. Prospective Utility: A New Interpretation of the Utility Requirement of Section 101 of the Patent Act. **California Law Review**, v. 87, n. 2, p. 423-436, 1999.

MADALENA, Juliano. Comentários ao Marco Civil da Internet - Lei 12.965, de 23 de abril de 2014. **Revista de Direito do Consumidor**, v. 94, p. 332, jul./ago. 2014.

MADDEN, Mary. **Privacy management on social media sites**. A Project of the Pew Research Center. Disponível em: <http://www.isaca.org/Groups/Professional-English/privacy-data-protection/GroupDocuments/PIP_Privacy%20mgt%20on%20social%20media%20sites%20Feb%202012.pdf>. Acesso em: 07 fev. 2016.

MADDOX, Teena. Wearables have a dirty little secret: 50% of users lose interest. **Tech Republic**, 13 fev. 2014. Disponível em: <http://www.techrepublic.com/article/wearables-have-a-dirty-little-secret-most-people-lose-interest/>. Acesso em: 30 jan. 2017.

MAGRANI, Eduardo. **Democracia Conectada** - A Internet como Ferramenta de Engajamento Político-Democrático. Curitiba: Juruá, 2014.

MAGRANI, Bruno et al. **Direitos Intelectuais**, 2014. Disponível em: <https://direitorio.fgv.br/sites/direitorio.fgv.br/files/u100/direitos_intelectuais_2014-2.pdf>. Acesso em: 29 mar. 2017.

MARKOFF, John. Entrepreneurs See a Web Guided by Common Sense. **The New York Times**, nov. 2006. Disponível em: <http://www.nytimes.com/2006/11/12/business/12web.html>. Acesso em: 27 mar. 2017.

MARX, Leo. Technology: The Emergence of a Hazardous Concept. **Technology and Culture**, vol. 51, n. 3, p. 561-577, 2010.

MATOSO, Filipe. Dilma diz que privacidade na Internet deve ter tratamento prioritário na ONU. **G1,** Brasília, 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/11/dilma-diz-que-privacidade-na-Internet-deve-ter-tratamento-prioritario-na-onu.html>. Acesso em: 07 fev. 2017.

MATTERN, Friedemann; FLOERKEMEIER, Christian. **From the Internet of Computers to the Internet of Things**. [s.d.]. Disponível em: <http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf>. Acesso em: 29 mar. 2017.

MCAFEE LABS. **Previsões sobre ameaças em 2017**. nov. 2016, p. 22. Disponível em: <https://www.mcafee.com/br/resources/reports/rp-threats-predictions-2017.pdf>. Acesso em: 24 fev. 2017.

MCCARTNEY, Scott. Viajante já pode testar aeroporto do futuro. **The Wall Street Journal**, jul. 2015. Disponível em: <http://br.wsj.com/articles/SB10836069722506714001504581112653322311690?tesla=y>. Acesso em: 25 jan. 2017.

MCDONALD, A. M.; CRANOR, L. F. The cost of reading privacy policies. **I/S: A Journal of Law and Policy for the Information Society,** v. 4, n. 3, p. 543-568, 2008.

MCNULTY, Eileen. Understanding Big Data: The Seven V's. **Dataconomy**, 22 mai. 2014. Disponível em: <http://dataconomy.com/2014/05/seven-vs-big-data/>. Acesso em: 27 mar. 2017.

MEDAGLIA, Carlo Maria; SERBANATI, Alexandru. **An Overview of Privacy and Security Issues in The Internet of Things**. Apresentado no vigésimo workshop de comunicações digitais, 2010.

MEIRA, Silvio. SINAIS do FUTURO IMEDIATO, #1: Internet das coisas. **ikewai**, Recife, dez. 2016. Disponível em:

<http://www.ikewai.com/WordPress/2016/12/12/sinais-do-futuro-imediato-1-Internet-das-coisas/>. Acesso em: 27 mar. 2017.

MEOLA, Andrew. How the Internet of Things will affect security & privacy. **Business Insider**, 19 dez. 2016. Disponível em: <http://www.businessinsider.com/Internet-of-things-security-privacy-2016-8>. Acesso em: 31 jan. 2017.

MILES, Stuart. Internet of Cows is now a thing as UK start-up creates cow tracking app. **Pocket-lint**, fev. 2016. Disponível em: <http://www.pocket-lint.com/news/136825-Internet-of-cows-is-now-a-thing-as-uk-start-up-creates-cow-tracking-app>. Acesso em: 25 jan. 2017.

MILL, John Stuart. **O utilitarismo**. São Paulo: Iluminuras, 2000

MILLER, Georgia e KEARNES, Matthew. **Nanotechnology, Ubiquitous Computing and The Internet of Things**: Challenges to Rights to privacy and data protection. Draft Report to the Council of Europe, set. 2013.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO. Marco Civil da Internet pode impedir acesso à inovação e geração de emprego, diz secretário. **Ministério da Ciência, Tecnologia e Inovação**, 2016. Disponível em: <http://www.mcti.gov.br/noticia/-/asset_publisher/epbV0pr6eIS0/content/marco-civil-da-Internet-pode-impedir-acesso-a-inovacao-e-geracao-de-emprego-diz-secretario>. Acesso em: 21 fev. 2017.

MIORANDI, Daniele et al. Internet of things: Vision, applications and research challenges. **Ad Hoc Networks,** vol. 10, 2012.

MITTELSTADT, Brent, et al. **The ethics of algorithms***:* Mapping the debate. Big Data & Society July–December 2016.

MOREIRA, Rafael. Em que atividades se concentram as empresas de serviços? **Economia de Serviços**, jun. 2016. Disponível em: <http://economiadeservicos.com/tag/estrutura-do-setor-de-servicos/>. Acesso em: 02 mai. 2017.

MOLARO, Cristian. Do not Ignore Structured Data in Big Data Analytics: the important role of structured data when gleaning information from Big Data. **IBM Big Data & Analytics Hub**, 19 jul. 2013. Disponível em: <**Error! Hyperlink reference not valid.** Disponível em: http://www.ibmbigdatahub.com/blog/do-not-ignore-structured-data-big-data-analytics>. Acesso em: 27 mar. 2017.

MORAES, Maria Celina Bodin de. Biografias não autorizadas: conflito entre a liberdade de expressão e a privacidade das pessoas humanas? Editorial. **Civilistica.com**, Rio de Janeiro, v. 2, n. 2, p. 1-4, 2013

MULHOLLAND, Caitlin Sampaio. **A responsabilidade civil por presunção de causalidade**. Rio de Janeiro: GZ, 2009.

MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. **Civilistica.com**, Rio de Janeiro, v. 1, n. 1, p. 1-11, 2012

MÜLLER, Leonardo. Tay: Twitter conseguiu corromper a IA da Microsoft em menos de 24 horas. **TecMundo**, mar. 2016. Disponível em: <https://www.tecmundo.com.br/inteligencia-artificial/102782-tay-twitter-conseguiu-corromper-ia-microsoft-24-horas.htm>. Acesso em: 16 ago. 2017.

NASCIMENTO Rodrigo, O que, de fato, é Internet das coisas e que revolução ela pode trazer? **Computerworld**, 12 mar. 2015. Disponível em: <http://computerworld.com.br/negocios/2015/03/12/o-que-de-fato-e-Internet-das-coisas-e-que-revolucao-ela-pode-trazer/>. Acesso em: 29 mar. 2017.

NAT'L INST. Health Services Research and the HIPAA Privacy Rule, **HIPAA Privacy Rules for Researchers**, mai. 2015. Disponível em: <https://privacyruleandresearch.nih.gov/pdf/healthservicesresearchhipaaprivacyrule.pdf>. Acesso em: 31 mar. 2017.

NISSENBAUM, Helen. **The Meaning of Anonymity in an Information Age.** The Information Society, 15:141-144, 1999.

NORDÅS, Hildegunn Kyvik; KIM, Yunhee. The Role of Services for Competitiveness in Manufacturing. **OECD Trade Policy Papers**, n. 148, 2013. Disponível em: <http://dx.doi.org/10.1787/5k484xb7cx6b-en>. Acesso em: 29 mar. 2017.

NORER, Roland (Ed.). **Genetic Technology and Food Safety**. New York: Springer, 2016.

O'BRIEN, Ciara. Wearables: Samsung chases fitness fans with Gear Fit 2. **The Irish Times**, 22 ago. 2016. Disponível em: <http://www.irishtimes.com/business/technology/wearables-samsung-chases-fitness-fans-with-gear-fit-2-1.2763512>. Acesso em: 29 mar. 2017.

O'REILLY, Tim. Design Patterns and Business Models for the Next Generation of Software. **O'Reilly**, set. 2005. Disponível em: <http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1>. Acesso em: 27 mar. 2017.

_____. Not 2.0? **Radar**, ago. 2005. Disponível em: <http://radar.oreilly.com/2005/08/not-20.html>. Acesso em: 28 mar. 2017.

O GLOBO. Samsung adverte: Cuidado com o que você diz em frente a sua TV inteligente. **O Globo**, 09 fev. 2015. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/samsung-adverte-cuidado-com-que-voce-diz-em-frente-sua-tv-inteligente-15286181> Acesso em: 30 mar. 2017.

OBAR, J. A.; OELDORF-HIRSCH, A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. In: **The 44th Research Conference on Communication, Information and Internet Policy,** 2016, p. 10-22. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465>. Acesso em: 28 set 2017.

OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review**, v. 57, p. 1701-1777, 2010.

OLDENZIEL, R. Introduction: Signifying Semantics for a History of Technology: **Technology and Culture**, v. 47, n. 3, p. 477-485, jul. 2006. Disponível em: <http://www.jstor.org/tc/accept?origin=/stable/pdf/40061168.pdf>. Acesso em: 05 jan. 2017.

OLHAR DIGITAL. Qual a diferença entre Internet e web? **Olhar Digital**, mar. 2014. Disponível em: <http://olhardigital.uol.com.br/noticia/qual-a-diferenca-entre-Internet-e-web/40770>. Acesso em: 27 mar. 2017.

OLIVEIRA, Márcio. Em marketing, Big Data não é sobre dados, é sobre pessoas! **Exame**, out. 2016. Disponível em: <http://exame.abril.com.br/blog/relacionamento-antes-do-marketing/em-marketing-bigdata-nao-e-sobre-dados-e-sobre-pessoas/>. Acesso em: 31 jan. 2017.

O QUE É Gopher? **Canal Tech**, [s.d.]. Disponível em: <https://canaltech.com.br/produtos/O-que-e-Gopher/>. Acesso em: 17 jul. 2017.

ORO, David. Bytes and Bushels - Farming on an Industrial Scale. **IoT Central**, set. 2015. Disponível em: <http://www.iotcentral.io/blog/bytes-and-bushels-farming-on-an-industrial-scale?context=tag-farming>. Acesso em: 25 jan. 2017.

OTTERLO, Van. A machine learning view on profiling. In: Hildebrandt M and de Vries K (eds) **Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology**. Abingdon: Routledge, pp. 41–64.

PAGALLO, Ugo. **The Laws of Robots**: Crimes, Contracts, and Torts. Torino: Springer, 2013.

_____; BAYAMLIOĞLU, Emre. **On the legal implications of regulation by technology**: of law and things. 2015.

PARISER, E. **The Filter Bubble**: What the Internet Is Hiding from You. New York: Penguin Press, 2011.

PARIKKA, Jussi; TIAINEN, Milla. **What is New Materialism.** Opening words from the event New Materialisms and Digital Culture. Anglia Ruskin University, 21-22 June 2010.

PASQUALE, F. **The Black Box Society:** The secret algorithms that control money and information. Harvard University Press. 2015

PATEL, Karan. Incremental Journey for World Wide Web: Introduced with Web 1.0 to Recent Web 5.0 – A Survey Paper. **International Journal of Advanced Research in Computer Science and Software Engineering**, v. 3, n. 10, p. 410-417, out. 2013.

PAYÃO, Felipe. Quebrando a Internet: estamos sofrendo o maior ataque DDoS da história. **Tecmundo**, 21 out. 2016. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/110842-grande-ataque-ddos-afeta-twitter-psn-spotify-outros-estragos.htm>. Acesso em: 30 mar. 2017.

PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. **Texas Law Review**, v. 93, p. 117-120, 2014.

PHILPOTT, Jeremy. Patents. In: _____; JOLLY, Adam. (Eds.). **A handbook of intellectual property management**: protecting, developing and exploiting your IP assets. London: The Patent Office/BTG, 2004.

PINOCHET, Luis Herman Contreras. **Tecnologia da informação e comunicação**. Rio de Janeiro: Elsevier, 2014.

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/smartwork-blog/ghost-iot-yet-come-Internet-insecure-things-2017>. Acesso em: 31 jan. 2017.

POIKOLA, Antti; KUIKKANIEMI, Kai; HONKO, Harri. MyData - A Nordic Model for human-centered personal data management and processing. **Ministry of Transport**

and Communications, [s.d.], p. 3. Disponível em: <https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/>. Acesso em: 28 set. 2017.

PONTIN, Jason. ETC: Bill Joy's Six Webs. **MIT Technology Review**, 29 Set. 2005. Disponível em: <http://www.technologyreview.com/view/404694/etc-bill-joys-six-webs/>. Acesso em: 29 mar. 2017.

PORTAL BRASIL. Microfone detecta arrombamentos e disparos de armas. **Portal Brasil**, abr. 2014. Disponível em: <http://www.brasil.gov.br/ciencia-e-tecnologia/2014/04/microfone-detecta-arrombamentos-e-disparos-de-armas>. Acesso em: 25 jan. 2017.

POSNER, Richard. *Economic Analysis of Law*. Chicago, 2014.

POWLES, Julia; JUDGE, Jenny. Internet das coisas ou das pessoas? Tradução por ZANATTA, Rafael A. F. **Outras palavras**, 27 mai. 2016. Disponível em: <http://outraspalavras.net/posts/377086/>. Acesso em: 31 jan. 2017.

PRADO, Eduardo. A Internet das Coisas terá um papel fundamental nas Cidades Inteligentes. **Convergência Digital**, abr. 2015. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=38476&sid=15>. Acesso em: 25 jan. 2017.

PRECISION FARMING to control irrigation and improve fertilization strategies on corn crops. **Libelium**, set. 1016. Disponível em: <http://www.libelium.com/precision-farming-to-control-irrigation-and-improve-fertilization-strategies-on-corn-crops/> Acesso em: 25 jan. 2017.

PRESCOTT, Roberta. Internet das coisas demanda boas práticas e não regulação prévia. **Associação Brasileira de Internet**, 2015. Disponível em: <http://www.abranet.org.br/Noticias/Internet-das-coisas-demanda-boas-praticas-e-nao-regulacao-previa-830.html#.WKyJFG8rLct>. Acesso em: 21 fev. 2016.

PROMONTORY. **EU GDPR:** A Primer. 19 fev. 2016. Disponível em: <http://www.promontory.com/News.aspx?id=4127>. Acesso em: 07 mar. 2017.

PURDY, Mark; DAVARZANI, Ladan; OVANESSOFF, Armen. Como a Internet das Coisas pode levar à próxima onda de crescimento no Brasil. **Harvard Business Review Brasil**, nov. 2015. Disponível em <http://hbrbr.com.br/como-a-Internet-das-coisas-pode-levar-a-proxima-onda-de-crescimento-no-brasil/>. Acesso em 28 jun. 2016.

QUAN-HAASE, Anabel; WELLMAN, Barry. Hyperconnected Net Work: Computer-Mediated Community in a High-Tech Organization. In: ADLER, Paul S.; HECKSCHER, Charles. **Towards Collaborative Community**. p. 281-333. Disponível em: <http://groups.chass.utoronto.ca/netlab/wp-content/uploads/2012/05/Hyperconnected-Net-Work.pdf>. Acesso em: 27 mar. 2017.

RADOMIROVIC, S. **Towards a Model for Security and Privacy in the Internet of Things**. 1st International Workshop on the Security of the Internet of Things, Tóquio, 2010.

RAWLS, John. **A Theory of Justice**. Harvard, 1971.

_____. **Uma teoria da justiça**. Trad. Almiro Pisetta e Lenita Maria Rimoli Esteves. 2. ed. São Paulo: Martins Fontes, 2002

RAY, Kate. Web 3.0. **Vimeo**, mai. 2010. Disponível em: <https://vimeo.com/11529540>. Acesso em: 27 mar. 2017.

REDAÇÃO. Varejista norte-americana descobre até gravidez de clientes com a ajuda de software. **Olhar Digital,** fev. 2012. Disponível em: <https://olhardigital.com.br/noticia/varejista-norte-americana-descobre-gravidez-de-clientes-com-a-ajuda-de-software/24231>. Acesso em: 25 set. 2017.

REDAÇÃO ADNEWS. Samsung usa tecnologia para ajudar pessoas a superarem medos. **Exame**, 02 jan. 2017. Disponível em: <http://exame.abril.com.br/marketing/samsung-usa-tecnologia-para-superar-medos/>. Acesso em: 27 mar. 2017.

REDAÇÃO OLHAR DIGITAL. 5 apostas para 2017 nos principais setores da tecnologia. **Olhar Digital**, 02 jan. 2017. Disponível em: <http://olhardigital.uol.com.br/noticia/5-apostas-para-2017-nos-principais-setores-da-tecnologia/65013>. Acesso em: 27 mar. 2017.

REDAÇÃO. Bruno Latour: "O objetivo da ciência não é produzir verdade indiscutíveis, mas discutíveis". **Diálogos R7**, 11 mar. 2017. Disponível em: <http://www.correiodopovo.com.br/blogs/dialogos/2017/03/1005/bruno-latour-o-objetivo-da-ciencia-nao-e-produzir-verdade-indiscutiveis-mas-discutiveisblb/>. Acesso em: 07 ago. 2017.

REUTERS. Programa de inteligência artificial da Microsoft causa novos problemas. **G1**, mar. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/03/programa-de-inteligencia-artificial-da-microsoft-causa-novos-problemas.html>. Acesso em: 16 ago. 2017.

RFID-COE. **O que é RFID**, [s.d.]. Disponível em: <http://www.rfid-coe.com.br/_Portugues/OqueERFID.aspx>. Acesso em: 29 mar. 2017.

RIBEIRO, Lígia Maria. **Algumas notas sobre a história da Internet,** Faculdade de Engenharia da Universidade do Porto, abr. 1998. Disponível em: <http://paginas.fe.up.pt/~mgi97018/historia.html>. Acesso em: 28 jul. 2017.

RIJMENAM, Mark van. Why the 3 V's are Not Sufficient to Describe Big Data. **DATAFLOQ**, ago. 2015. Disponível em: <https://datafloq.com/read/3vs-sufficient-describe-big-data/166>. Acesso em: 27 mar. 2017..

RODOTÀ, Stefano. **Assim o humano pode se defender do pós-humano**. Tradução de Danilo Doneda. 2015.

_____. **Il mondo nella rete: Quali i diritti, quali i vincoli**. Ed. Laterza. 2014.

_____. **Palestra**, Rio de Janeiro, 2003. Disponível em: <http://www.rio.rj.gov.br/dlstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf>. Acesso em: 31 mar. 2017.

_____. **Iperdemocrazia**. Ed. Laterza. 2013.

_____. **A vida na sociedade de vigilância** – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Alexandre; SANTOS, Priscilla. A ciência que faz você comprar mais. **Galileu,** [s.d.]. Disponível em:

<http://revistagalileu.globo.com/Revista/Common/0,,EMI317687-17579,00-A+CIENCIA+QUE+FAZ+VOCE+COMPRAR+MAIS.html>. Acesso em: 25 set. 2017.

RODRIGUEZ, Diogo Antonio. A era dos bots na política brasileira já começou. **Motherboard**, jul. 2017. Disponível em: <https://motherboard.vice.com/pt_br/article/xwzwba/a-era-dos-bots-na-politica-brasileira-ja-comecou>. Acesso em: 16 ago. 2017.

ROMAN, Rodrigo; NAJERA, Pablo; LOPEZ, Javier. Securing the Internet of Things. **IEEE Computer**, v. 44, p. 51-58, 2011.

_____; ZHOU, Jianying; LOPEZ, Javier. On the features and challenges of security and privacy in distributed Internet of things. **Computer Networks**, n. 57. p. 2266-2279, 2013.

ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. **The Internet of Things**: An Overview. Understanding the Issues and Challenges of a More Connected World. ISOC, 2015. Disponível em: <https://www.Internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf>. Acesso em: 30 mar. 2017.

ROSSOW, Mark P. **Ethics:** An Alternative Account of the Ford Pinto Case, 2015.

ROUANET, Sergio Paulo. **Mal-estar na modernidade.** São Paulo: Companhia das Letras, 1993.

RYAN, Johnny. **A history of the Internet and the digital future**. London: Reaktion Books, 2010.

RÜDIGER, Francisco. Breve história do pós-humanismo: elementos de genealogia e criticismo. **Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação**, v. 8, p. 6, abr. 2007.

SANCHEZ VASQUEZ, Adolfo. **Ética.** 14. ed. Rio de Janeiro: Civilizacao Brasileira, 1993.

SANDEL, Michael. Justiça. **O que é fazer a coisa certa?**. Civilização Brasileira. Rio de janeiro, 2009.

SANTOS, Adriana B. A. dos; FAZION Cíntia B.; MEROE, Giuliano P. S. de. Inovação: Um Estudo sobre a evolução do conceito de Schumpeter. **Revista Caderno de Administração da Faculdade de Administração da FEA PUC/SP**, São Paulo, v. 5, n. 1, 2011. Disponível em: <http://revistas.pucsp.br/index.php/caadm/article/view/9014>. Acesso em: 27 mar. 2017.

SANTOS, Boaventura de Souza. **Pela mão de Alice**: O social e o político na pós-modernidade. 7. ed. Porto: Edições Afrontamento, 1999.

_____. **A nova Tese Treza.** 2018. Disponível em: <http://outraspalavras.net/capa/boaventura-a-nova-tese-onze/>. Acesso em: 29 set. 2017.

SANTOS, Maike Wile dos. O Big Data somos nós: a humanidade de nossos dados. **Jota**, 16 mar. 2017. Disponível em: <https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-big-data-somos-nos-a-humanidade-de-nossos-dados-16032017>. Acesso em: 27 mar. 2017.

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, Setúbal, 2016.

SANTUCCI, Gérald. **The Internet of Things**: Between the Revolution of the Internet and the Metamorphosis of Objects. Disponível em: <http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-between-the-Internet-revolution.pdf>. Acesso em: 29 mar. 2017.

SARAIVA, Leonardo. **Sistema de Análise de Erros Humanos na Prevenção De Acidentes Aeronáuticos.** 2011.

SARLET, Ingo Wolfgang**. Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988.** Porto Alegre: Livraria do Advogado, 2001.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional.** São Paulo: Editora Revista dos Tribunais, 2012

SAURWEIN, Florian; JUST, Natascha; LATZER, Michael. **Governance of algorithms:** options and limitations. Info, v. 17, n. 6, p. 35-49, 2015.

SCHATZBERG, Eric. From art to applied science. **Isis**, v. 103, n. 3, p. 555-563, 2012.

_____. Technik Comes to America: Changing Meanings of Technology before 1930. **Technology and Culture**, v. 47, n. 3, p. 486-512, jul. 2006. Disponível em: <http://muse.jhu.edu/article/201479>. Acesso em 27 mar. 2017.

SCHMIDT, Eric; COHEN, Jared. **The new digital age: Reshaping the future of people, nations and business**. Londres: Hachette UK, 2013.

SCHWAB, Klaus. **The Fourth Industrial Revolution**. Cologny/Geneva: World Economic Forum, 2016.

SHADBOLT, Nigel; HALL, Wendy; BERNERS-LEE, Tim. The Semantic Web Revisited. **IEEE Computer Society**, p. 96-101, mai/jun. 2006. Disponível em: <http://eprints.soton.ac.uk/262614/1/Semantic_Web_Revisted.pdf>. Acesso em: 28 mar. 2017.

SHANNON, Victoria. A 'more revolutionary' web. **The New York Times**, mai. 2006. Disponível em: <http://www.nytimes.com/2006/05/23/technology/23iht-web.html>. Acesso em: 28 mar. 2017.

SICARI, S. et al. Security, privacy and trust in Internet of Things: The road ahead. **Computer Networks**, v. 76, 2015.

SJÖBERG, Mats et al. Digital Me: Controlling and Making Sense of My Digital Footprint. In: GAMBERINI, L. et al (Eds.). **Symbiotic Interaction:** Lecture notes in computer science. Padua: Springer, 2016.

SKARMETA, Antonio, RAMOS José; MORENO, Victoria. **A decentralized approach for security and privacy challenges in the Internet of Things**. Apresentado no IEE World Forum, 2014.

SLOAN, Robert H.; WARNER, Richard. **Unauthorized Access:** The Crisis in Online Privacy and Security. London/New York: CRC Press, 2014.

SLOWEY, Lynne. AT&T and IBM partner for analytics with Watson. **IBM**, mar. 2017. Disponível em: <https://www.ibm.com/blogs/cloud-computing/2017/03/att-ibm-analytics-watson/>. Acesso em: 28 abr. 2017

SMARTWATCH OWNERSHIP rises at a quick pace, activity tracker ownership has begun to plateau. **Wearables Authority**, 13 jul. 2015. Disponível em: <http://authoritywearables.com/smartwatch-ownership-rises-at-a-quick-pace-activity-tracker-ownership-has-begun-to-plateau>. Acesso em: 31 jan. 2017.

SMITH IV, Jack. Press This Button and Something Will Happen on the Internet. **Observer**, jan. 2015. Disponível em: <http://observer.com/2015/01/press-this-button-and-something-will-happen-on-the-Internet/>. Acesso em: 25 jan. 2017.

SOLOVE, Daniel. A Taxonomy of Privacy. **University of Pennsylvania Law Review**. v. 154, n. 3, p. 477-560, 2006.

SOUZA, Carlos Affonso Pereira de. O progresso tecnológico e a tutela jurídica da privacidade, **Direito, Estado e Sociedade**, n. 16, p. 8, jan./jul. 2000

STACKOWIAK, Robert et al. Big Data and the Internet of Things: **Enterprise Information Architecture for a New Age**. Nova York: Apress, 2015.

STAUDENMAIER, John M. Recent Trends in the History of Technology. **The American Historical Review**, v. 95, n. 3, p. 715-725, jun. 1990.

STIEBEN, Danny. The Archie search engine – the world's first search! **Make Use Of**, may. 2013. Disponível em: <http://www.makeuseof.com/tag/the-archie-search-engine-the-worlds-first-search/>. Acesso em 17 jul. 2017.

STONE, Brad. **The Everything Store**: Jeff Bezos and the Age of Amazon. Boston: Little Brown and Company, 2013.

SUMARES, Gustavo. Facebook desativa inteligência artificial que criou linguagem própria. **Olhar Digital**, jul. 2017. Disponível em: <https://olhardigital.com.br/noticia/facebook-desativa-inteligencia-artificial-apos-ela-criar-sua-propria-linguagem/70075>. Acesso em: 16 ago. 2017.

_____. Sistema do Google inventou uma língua própria que humanos não entendem. **Olhar Digital**, nov. 2016. Disponível em: <https://olhardigital.com.br/pro/noticia/sistema-do-google-inventou-uma-lingua-propria-que-humanos-nao-entendem/64122>. Acesso em: 16 ago. 2017.

TECHTARGET ANZ STAFF. What is hyperconnectivity? **Computer weekly**, 19 fev. 2007. Disponível em: <http://www.computerweekly.com/news/2240100953/What-is-hyperconnectivity>. Acesso em: 27 mar. 2017.

THE 2016 IMD World: competitiveness scoreboard. 2016. Disponível em <http://www.imd.org/uupload/imd.website/wcc/scoreboard.pdf>. Acesso em: 28 jun. 2016.

THE GUARDIAN. DDoS attack that disrupted Internet was largest of its kind in history, experts say. **The Guardian**, out. 2016. Disponível em: <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>. Acesso em: 30 mar. 2017.

THE INTERNET of Things is Actually full of Useless Things. **Next Big What**, 6 fev. 2015. Disponível em: <https://www.nextbigwhat.com/Internet-of-useless-things-297/>. Acesso em: 31 jan. 2017.

THE LEMELSON-MIT PROGRAM. **Historical perspectives on inventions & creativity**. Workshop realizado pela escola de engenharia do MIT (Massachusetts Institute of Technology), 2003. Disponível em:

<http://web.mit.edu/monicaru/Public/old%20stuff/For%20Dava/Grad%20Library.Data/PDF/history-3289136129/history.pdf>. Acesso em: 28 mar. 2017.

THE TESLA IOT Car: Case Study. **MITCNC Blog**, ago. 2014. Disponível em: <https://blogmitcnc.org/2014/08/21/the-tesla-iot-car-case-study/>. Acesso em: 25 jan. 2017.

TOTLAB. O que é TIC? **TotLab**, mai 2012. Disponível em: <http://totlab.com.br/noticias/o-que-e-tic-tecnologias-da-informacao-e-comunicacao/>. Acesso em: 31 mar. 2017.

TRIGUEIRO, Michelangelo Giotto Santoro. O que foi feito de Kuhn? O construtivismo na Sociologia da Ciência: considerações sobre a prática das novas biotecnologias. In: SOBRAL, Fernanda et al. (orgs.) **A alavanca de Arquimedes** – ciência e tecnologia na virada do século. Brasília: Paralelo 15, 1997.

UCKELMANN, Dieter; HARRISON, Mark; MICHAHELLES, Florian. **Architecting the internet of things.** Berlim: Springer, 2011.

UM CAMPUS ABERTO à pesquisa e testes para mercado de IoT. **Inatel**, set. 2016. Disponível em: <http://www.inatel.br/imprensa/noticias/pesquisa-e-inovacao/2938-um-campus-aberto-a-pesquisa-e-testes-para-mercado-de-iot>. Acesso em: 25 jan. 2017.

VAN DEURSEN, T. 50 Ways to Break RFID Privacy. Privacy and Identity Management for Life, **IFIP Advances in Information and Communication Technology**, v. 352, p. 192-205, 2011.

VEJA COMO a tecnologia pode deixar a sua casa mais segura. **Olhar Digital**, 02 jan. 2017. Disponível em: <**Error! Hyperlink reference not valid.**http://olhardigital.uol.com.br/lu-explica/noticia/veja-como-a-tecnologia-pode-deixar-a-sua-casa-mais-segura/64971>. Acesso em: 27 mar. 2017.

VENTURINI, Jamila et. al. **Terms of Service and Human Rights:** an analysis of online platform contracts. Rio de Janeiro: Revan, 2016

VERASZTO, Estéfano Vizconde et al. Tecnologia: Buscando uma definição para o conceito. **PRISMA.COM**, n. 7, p. 60-85, 2008. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/viewFile/681/pdf>. Acesso em: 02 mai. 2017.

VERBEEK, Peter. **Moralizing Technology:** Understanding and Designing the Morality of Things, Chicago - London, The University of Chicago Press. 2011.

VLADECK, David C. Machines without principals: liability rules and artificial intelligence. **Washington Law Review**, vol. 89, n. 1, mar. 2014.

WAHER, Peter. **Learning internet of things.** Birmingham: Packt Publishing Ltd, 2015.

WALLACE, K.A. **Anonymity.** Ethics and Information Technology 1 (1), 23-35. 1999.

_____. **On-line Anonymity**. Entry for Handbook on Information and Computer Ethics, eds. Herman Tavani and Ken Himma, John Wiley & Sons, Inc., 165-189. 2008.

WALLACH, Wendell, et al. *Artificial Intelligencefor the Common Good Sustainable*, Inclusive and Trustworthy. 2017. Disponível em: <https://weforum.ent.box.com/v/AI4Good?platform=hootsuite>. Acesso em: 28 fev. 2017.

WALLACH, Wendell; ALLEN Colin. **Moral Machines:** Teaching Robots Right from Wrong, Oxford University Press, 2008.

WANG, Yongheng; ZHANG, Xiaoming (Ed.). **Internet of Things:** International Workshop, IOT 2012, Changsha, China, August 17-19, 2012. Nova York: Springer, 2012.

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

WEB 3.0 & Beyond. **Rad Students Wiki**, [20--]. Disponível em: <http://rad-students.wikia.com/wiki/Web_3.0_%26_Beyond>. Acesso em: 28 mar. 2017.

WEBER, Rolf H. Internet of Things – New security and privacy challenges. **Computer Law & Security Review**, n. 26. p. 23-30, 2010.

WEINBERG, Darin. Social Constructionism. In: Bryan S. Turner (Ed.). **The new blackwell companion to social theory.** Chichester, UK: Wiley-Blackwell, 2009.

WEINMAN, Joe. **Digital Disciplines:** Attaining Market Leadership via the Cloud, Big Data, Mobility, Social Media, and the Internet of Everything. Hoboken: John Wiley & Sons, 2015.

WEISSBERGER, Alan. Are the Internet of Things (IoT) & Internet of Everything (IoE) the Same Thing? **VIODI**, mai. 2014. Disponível em: <http://viodi.com/2014/05/23/are-the-Internet-of-things-iot-Internet-of-everything-iot-the-same-thing/>. Acesso em: 28 mar. 2017.

WENTZEL, Marina. 'Quarta revolução industrial': Como o Brasil pode se preparar para a economia do futuro. **BBC Brasil**, jan. 2016. Disponível em: <http://www.bbc.com/portuguese/noticias/2016/01/160122_quarta_revolucao_industrial_mw_ab>. Acesso em: 28 mar. 2017.

WILLIAMS, Clarence. Hackers hit D.C. police closed-circuit camera network, city officials disclose. **The Washington Post**, 27 jan. 2017. Disponível em: <https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.3dc5da77508f> Acesso em: 30 mar. 2017.

WOLF, Marty, et al. **Why We Should Have Seen That Coming***:* Comments on Microsoft's tay "Experiment," and Wider Implications. 2017. Disponível em: <http://digitalcommons.sacredheart.edu/computersci_fac/102/>. Acesso em 27 set. 2017.

WU, Tim. **The Master Switch:** The Rise and Fall of Information Empires. Vintage. 2011

ZANATTA, Rafael A. F. Internet das Coisas: privacidade e segurança na perspectiva dos consumidores [Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017] – **Instituto Brasileiro de Defesa do Consumidor**, 2017.

_____. **O Utilitarismo de Jeremy Bentham.** 2010. Disponível em: <https://rafazanatta.blogspot.com.br/2010/04/o-utilitarismo-de-jeremy-bentham.html>. Disponível em: 20 set. 2017.

ZIEGELDORF Jan; MORCHON, Oscar; WEHRLE, Klaus. Privacy in the Internet of Things: Threats and Challenges. **Revista Security and Communication Networks**, v. 7, n. 12, p. 2728- 2742, 2013.

LINKS UTILIZADOS:

https://www.youtube.com/watch?v=46hEaFKa638
http://www.computersciencezone.org/wp-content/uploads/2015/04/Security-and-the-Internet-of-Things.jpg#sthash.c6u2POMr.dpuf
https://www.youtube.com/watch?v=jlkvzcG1UMk.
http://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-Internet-of-things/.
http://www.wired.com/2014/11/the-Internet-of-things-bigger/
http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf
http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-between-the-Internet-revolution.pdf
http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
http://www.Internetsociety.org/Internet/what-Internet/history-Internet/brief-history-Internet
http://www.technologyreview.com/view/404694/etc-bill-joys-six-webs/
http://www.cio.com/article/2438016/infrastructure/20-years-of-it-history--connecting-devices--data-and-people.html
http://www.rfidjournal.com/articles/view?4986
http://www.rfid.ind.br/Internet-das-coisas#.VagXS_lVhHw
http://www.rfid-coe.com.br/_Portugues/OqueERFID.aspx
http://www.gradeti.com.br/blog/rfid/2014/07/rfid-e-privacidade-experiencias-derrubam-alguns-mitos/
http://www.differencebetween.com/difference-between-rfid-and-vs-bluetooth/
http://www.differencebetween.com/difference-between-rfid-and-vs-bluetooth/
https://www.youtube.com/watch?v=EMkTic4ztU8
http://www.practicalecommerce.com/articles/464-Basic-Definitions-Web-1-0-Web-2-0-Web-3-0
http://conferences.oreillynet.com/web2con/
http://airccse.org/journal/ijwest/papers/3112ijwest01.pdf
http://www.ris.uvt.ro/wp-content/uploads/2009/01/giurgiubirsan.pdf
http://firstmonday.org/ojs/index.php/fm/article/view/2125/1972
http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1
https://vimeo.com/11529540
http://www.nytimes.com/2006/11/12/business/12web.html
http://www.nytimes.com/2006/05/23/technology/23iht-web.html
http://www.cs.umd.edu/~golbeck/LBSC690/SemanticWeb.html
http://eprints.soton.ac.uk/262614/1/Semantic_Web_Revisted.pdf
http://lifeboat.com/ex/web.3.0
http://time.com/539/the-next-big-thing-for-tech-the-Internet-of-everything/
http://viodi.com/2014/05/23/are-the-Internet-of-things-iot-Internet-of-everything-iot-the-same-thing/
http://www.ijarcsse.com/docs/papers/Volume_3/10_October2013/V3I10-0149.pdf
http://radar.oreilly.com/2005/08/not-20.html
http://meiobit.com/297796/ptc-tech-day-mostra-a-verdadeira-Internet-das-coisas/
http://computerworld.com.br/negocios/2015/03/12/o-que-de-fato-e-Internet-das-coisas-e-que-revolucao-ela-pode-trazer
http://www.mail-archive.com/bib_virtual@ibict.br/msg01199.html
http://airccse.org/journal/ijwest/papers/3112ijwest01.pdf
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12715.htm
http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=36637&sid=8
https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/decreto/d8234.htm
http://www.tirio.org.br/info/35868/governo-adia-mais-uma-vez-megapiloto-de-Internet-das-coisas-no-pais

http://computerworld.com.br/iot-pode-agregar-us-352-bilhoes-economia-brasileira-ate-2022
http://www1.folha.uol.com.br/tec/2015/06/1636947-mercado-de-Internet-das-coisas-deve-triplicar-para-us17-tri-ate-2020-diz-idc.shtml
http://openinterconnect.org/members/
http://adrenaline.uol.com.br/2015/05/28/34858/google-confirma-o--project-brillo-sua-versao-do-android-para-a-Internet-das-coisas
http://www.infowester.com/big-data.php
http://br.wsj.com/articles/SB10836069722506714001504581112653322311690?tesla=y
http://br.wsj.com/articles/SB10836069722506714001504581112653322311690?tesla=y
http://meiobit.com/
http://trendwatching.com/trends/Internet-of-caring-things/
http://www.libelium.com/50_sensor_applications/
http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VZRsHflVhHw
http://info.abril.com.br/noticias/seguranca/2015/02/samsung-pede-que-clientes-evitem-discutir-assuntos-pessoais-em-frente-de-sua-smarttv.shtml
https://blog.kaspersky.com.br/pesquisa-como-hackear-minha-casa/3804/
http://cetic.br/media/docs/publicacoes/2/tic-domicilios-e-empresas-2012.pdf.
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
https://events.ccc.de/congress/2014/Fahrplan/events/6459.html
http://www.mc.gov.br/programa-nacional-de-banda-larga-pnbl.
https://support.google.com/youtube/answer/2797370?hl=pt-BR
https://en.wikipedia.org/wiki/Funk_carioca.
https://en.wikipedia.org/wiki/Tecno_brega.hHttp://www.cultura.gov.br/noticias-destaques//asset_publisher/OiKX3xlR9iTn/content/id/1248553.
http://www.tirio.org.br/info/36007/porque-a-Internet-das-coisas-implica-em-gerenciar-contextos-e-nao-dados
http://cetic.br/media/docs/publicacoes/2/TIC_DOM_EMP_2013_livro_eletronico.pdf
http://www.wirelessmundi.inf.br/edicao-n-13/1448-capa
http://g1.globo.com/jornal-da-globo/noticia/2014/11/Internet-das-coisas-permite-que-tudo-ao-nosso-redor-esteja-conectado.html
http://www.envolverde.com.br/ambiente/instituto-desenvolve-tecnologia-inovadora-para-deteccao-de-vazamento-de-agua-potavel/
http://zh.clicrbs.com.br/rs/noticias/noticia/2013/10/estudantes-criam-aplicativo-para-usuarios-de-onibus-de-porto-alegre-4289330.html
http://www.curitiba.pr.gov.br/noticias/paineis-em-terminais-informam-horario-do-onibus-em-tempo-real/31665
http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=38476&sid=15
http://www.brasil.gov.br/ciencia-e-tecnologia/2014/04/microfone-detecta-arrombamentos-e-disparos-de-armas
http://zh.clicrbs.com.br/rs/noticias/noticia/2013/04/projeto-pioneiro-no-brasil-botao-de-panico-ajuda-a-reduzir-violencia-no-es-4119173.html
http://www.nytimes.com/2006/11/12/business/12web.html?scp=1&sq=John%20Markoff%203.0&st=cse&_r=0