EDUARDO MAGRANI

entre dados e robôs

ÉTICA E PRIVACIDADE NA ERA DA HIPERCONECTIVIDADE

SÉRIE PAUTAS *em* DIREITO

EDUARDO MAGRANI

Entre dados e robôs

ÉTICA E PRIVACIDADE NA ERA DA HIPERCONECTIVIDADE

Capa
Brand&Book — Paola Manica e equipe

Revisão
Fernanda Lisbôa
Tito Montenegro

ARQUIPÉLAGO EDITORIAL LTDA.
Rua Hoffmann, 239/201
CEP 90220-170
Porto Alegre — RS
Telefone 51 3012-6975
www.arquipelago.com.br

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 ontoepistemológica *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 tímido-*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.

Sumário

Agradecimentos

Caitlin Sampaio | Sérgio Branco | Carlos Affonso | Danilo Doneda | Ronaldo Lemos | Cláudio Lucena | Luiz Abrahão | Renan Medeiros | Helena Ferreira | Eduardo Peixoto | Claudia Cunha | Fernanda Nunes | Júlia Costa | Walter Britto | Christian Djeffal | Christian Marks | Caio César de Oliveira | Bartira, Fabio e Sylvio Magrani | Ana Lucia, Cristina, Felipe e Bruno Magrani | Lucy Massa | Octavio, Tito e Caio Guedes | Adriana Bittencourt | Ana Lara Mangeth | Pedro Augusto Francisco | Fernando Lennertz | Chiara de Teffé | Luca Belli | Luã Fergus | Hugo Esteves

Colaboradores de Pesquisa:
Luiz Abrahão | Renan Medeiros | Helena Ferreira

Prefácio

I.

O mundo nos é oferecido sem concessões. Temos o espaço terreno e o tempo presente — e é tudo. Pode parecer pouco. Afinal, muitos foram os acontecimentos históricos que não testemunhamos (e outros tantos que não iremos testemunhar), e infinitos são os lugares em que nossa presença está física e tecnologicamente impossibilitada. Mas tentar dar conta de entender o aqui e o agora já é tarefa mais do que ambiciosa.

É isso que, sob certa perspectiva, tenta fazer o Direito: compreender o mundo para organizar o caos potencial de todas as coisas. Sempre a reboque da realidade, quase sempre atrasado em seu intento, o Direito tem por fim ser "a solução prudente dentro da ordem" (segundo José de Oliveira Ascensão) ou, ainda, "um conjunto de regras obrigatórias que garante a convivência social graças ao estabelecimento de limites à ação de cada um de seus membros" (para Miguel Reale).

A busca pelo equilíbrio entre a liberdade de ação e a regulação jurídica tem sido assim há séculos. E durante muito tempo foi possível viver uma vida inteira sob a certeza das condutas sociais esperadas e das regras a serem aplicadas. Uma vida inteira sem mudanças significativas na tecnologia circundante ou na sociedade em que o homem se encontrava imerso. Não é mais assim.

É provável que os maiores desafios da contemporaneidade ao Direito sejam a velocidade com que a tecnologia se desenvolve e as consequências desse progresso. Nesse particular, vivemos em um tempo/espaço particularmente fértil. E, se pudermos dizer que temos uma boa e uma má notícia para dar, é curioso que ambas sejam a mesma notícia: o avanço tecnológico só vai aumentar.

Esse prognóstico é sedutor porque nos permite experimentar, de verdade, o futuro outrora especulado, e isso é, sem dúvida, excitante. Entretanto, caberá ao Direito lidar com incertezas ainda maiores, permeadas por minudências técnicas, interdisciplinares e que colocarão sob escrutínio nossas certezas sobre direitos humanos, direitos de personalidade, privacidade, direitos autorais, direito contratual e o inesgotável campo da ética.

E, por tudo isso, não há momento melhor para se ler o livro de Eduardo Magrani.

II.

Toda obra que se proponha a apresentar uma tese tem a dupla tarefa de explicar e de iluminar. É preciso organizar o mundo das informações para mostrar ao leitor do que, exatamente, a tese se trata. É fundamental coletar e conectar informações, evidências, decisões, opiniões e normas jurídicas a fim de bem pavimentar o caminho que o leitor vai percorrer. Uma tese é, assim, um mapa. E, como todo mapa, para ser útil e servir ao propósito a que se destina, precisa conter todas as informações necessárias à compreensão do tema, mas apenas as informações necessárias à sua compreensão.

Além de mapa, a tese é guia. Ela precisa apontar para o futuro, sugerir novas veredas e soluções e, naturalmente, surpreender. A tese precisa ser estática e dinâmica, perene e flexível, contemporânea

e pós-contemporânea. Precisa evidenciar o que não é óbvio, fazer as conexões certas e, ambição suprema: ser de leitura agradável.

Por tudo isso mais, não há tese melhor para se ler neste momento do que a de Eduardo Magrani.

III.

Aqueles que têm agora ao menos 30 anos sabem, por seu próprio testemunho, o quanto a tecnologia vem imprimindo mudanças velozes no mundo em que vivemos. A tríade Internet das Coisas/*Big Data*/Inteligência Artificial promete transformar as relações sociais, e ainda é cedo para sabermos as verdadeiras consequências dessa transformação. Por isso o tema é urgente e por isso, também, é ousado.

As consequências da hiperconectividade já se fazem sentir. Questões relacionadas à privacidade, ao *social credit system* que vem sendo desenvolvido na China, à memória perpétua da internet e às suas implicações já são temas amplamente debatidos. Discussões sobre vigilância e abuso de poder digital não são mais apenas combustível para debater episódios de *Black Mirror*. Esses assuntos dizem respeito à vida que todos nós estamos vivendo bem agora.

Muito mais vem por aí. As implicações éticas relacionadas a robôs e o tratamento adequado ao estatuto jurídico de entes não humanos ainda são assuntos embrionários. A inteligência artificial será responsável pela usurpação de tarefas humanas? Haverá desemprego em massa? Criaremos classes distintas de seres humanos (alguns com mais dignidade do que outros)? Qual o papel do Direito e sua capacidade de regular este mundo cada vez mais invisivelmente técnico? É cedo para sabermos, mas Eduardo Magrani enfrenta esses

assuntos com profundidade e clareza, cumprindo com a promessa e o dever de cada tese: iluminando nossa compreensão.

A função de uma obra nunca é esgotar-se, pois que se trataria de função impossível. O sucesso de uma obra se mede pela capacidade de nos fazer pensar e de permitir a expansão do mapa que ela própria traçou. Eis aqui uma tese bem-sucedida.

IV.

Em *Fanny e Alexander*, sua obra mais pessoal, Ingmar Bergman afirma, no final do filme, que "tudo pode acontecer, tudo é possível e verossímil. O tempo e o espaço não existem. Em cima de um insignificativo fundo de realidade, a imaginação espraia-se e tece novos padrões".

Apesar de se tratar de uma produção de 1983, nunca essa afirmação pareceu tão verdadeira. Vivemos no mundo das infinitas possibilidades, onde a realidade e a imaginação trocam constantemente de lugar a fim de criar novas matrizes. Cabe a cada um de nós fazer o esforço diário de compreender e explicar nosso mundo — não só para nós mesmos, mas para nossos sucessores.

É por isso que toda contribuição de qualidade e profunda para a compreensão do mundo, especialmente quando o assunto é complexo e controvertido, é bem-vinda.

Diante de tantas possibilidades temporais e espaciais que caberiam a cada um de nós, diante de todos os séculos passados e futuros, de lugares distantes, inacessíveis ou impossíveis, que sorte temos de compartilhar esse mesmo tempo e esse mesmo espaço (quer de fato existam ou não) com Eduardo Magrani.

Sérgio Branco

Diretor do Instituto de Tecnologia e Sociedade
do Rio de Janeiro (ITS Rio)

Apresentação

Logo que ingressou no Programa de Doutorado da Pós-Graduação em Direito da PUC-Rio, Eduardo Magrani, muito animado, me chamou para uma conversa a respeito de um assunto que seria uma das grandes novidades da interseção entre Direito e Tecnologia: a Internet das Coisas. Intrigada, e ainda bastante ignorante sobre o tema, aceitei orientá-lo durante os seguintes anos de pesquisa. Confesso que, naquele momento inicial, a ideia de mergulhar numa investigação acadêmico-jurídica sobre bens conectados por rede me pareceu algo que muito se aproximava de uma ficção científica. Algo como um casamento entre *Star Trek* e *The Jetsons*. Mais enganada não poderia estar.

Ao ser apresentada ao assunto pelo Eduardo, percebi uma absoluta interlocução entre os temas do desenvolvimento tecnológico e dos direitos fundamentais, passando pela necessária discussão sobre os limites éticos do uso das tecnologias, tão relevante na atualidade para possibilitar uma regulação que caminha lado a lado com o aprimoramento tecnológico.

Já se sabe que a tecnologia se desenvolve a largos passos e que o Direito não consegue acompanhar o seu ritmo, de forma que a sua regulação deficiente revela, por vezes, um obstáculo para a plena proteção dos interesses existenciais da pessoa humana. É no âmbito da tecnologia conhecida como Internet das Coisas (ou *Internet of Things*, ou, ainda, IoT) que se revela um dos principais debates nesta área, qual seja, o que se refere à proteção da privacidade ou dos

dados pessoais que são disponibilizados e coletados por estas "coisas" conectadas, cada vez mais inteligentes e autônomas.

A Internet das Coisas representa inovação tecnológica que permite a criação de ambiente interligado através de sensores que conectam objetos ou bens por meio da internet, possibilitando não só a comunicação e realização de funções específicas entre as coisas, como gerando a cada vez mais constante coleta, transmissão, guarda e compartilhamento de dados entre os objetos e, consequentemente, entre as empresas que disponibilizam este tipo de tecnologia às pessoas.

Com a popularização da tecnologia IoT e a sua utilização frequente em objetos de nosso cotidiano — smartphones, televisores, relógios, pulseiras identificadoras de funções físicas e de saúde, tablets, dentre outros — o que se questiona, do ponto de vista do Direito, é se existe uma política eficiente de proteção dos dados e da privacidade das pessoas que utilizam tais objetos. E se, diante desta questão, as pessoas estariam dispostas a renunciar à proteção de seus dados em contrapartida aos benefícios evidentes que tal tecnologia gera em suas vidas, justificando esta troca com base numa conveniência pessoal evidente.

Deve-se considerar, nessa nova realidade tecnológica, que os dados de uma pessoa possuem, ao mesmo tempo, um caráter existencial que se revela preponderantemente na proteção da privacidade e da identidade da pessoa humana — em decorrência da tutela de sua dignidade —, e um caráter patrimonial, que se identifica pela possibilidade do uso desses dados como insumo para o desenvolvimento de atividades empresariais das mais diversas áreas. Trata-se, nesse caso, do que se definiu como monetização de dados, ou seja, a conversão de informações em dinheiro. Portanto, ao lado

de uma necessária proteção de situações jurídicas de natureza extrapatrimonial (privacidade, identidade, imagem), deve-se atentar que também é possível uma avaliação de natureza patrimonial desses mesmos dados, que, por sua vez, constituem parte fundamental do modelo de negócios desenvolvido por grandes atores do mercado de tecnologia.

Os temas enfrentados por Eduardo Magrani em sua pesquisa de Doutorado, que resultaram neste magnífico livro, são de absoluta relevância para a compreensão de como um fenômeno tecnológico pode impactar o exercício e a tutela de direitos fundamentais. Falar de Internet das Coisas hoje é necessariamente falar de proteção de dados pessoais e regulação de Inteligência Artificial. Ao considerarmos que o desenvolvimento da tecnologia IoT depende, sobremaneira, da forma como as coisas conectadas trocam entre si informações sobre dados pessoais coletados, percebemos aqui uma verdadeira necessidade de regular, de maneira responsável, o uso da tecnologia para impedir que ela seja usada como instrumento de violação de direitos fundamentais, tais como o direito à privacidade e o direito à identidade. O debate acerca da proteção da privacidade e, mais especificamente, da proteção de dados foi o fio condutor de sua pesquisa e uma verdadeira preocupação que permeou sua investigação sobre os limites da tecnologia frente à tutela de direitos humanos.

No desenvolvimento de seu livro, Eduardo Magrani buscou realizar não só uma conceituação precisa do fenômeno da Internet das Coisas, também correlacionou a regulação jurídica da tecnologia à necessária análise da ética, da proteção dos dados e da automação, num mundo tecnorregulado e em constante transformação a partir da interação entre homens e máquinas.

Esse é, portanto, um livro fundamental, cuja leitura se faz necessária por aqueles que pretendam compreender o fenômeno da Internet das Coisas e sua interlocução com as mais contemporâneas questões referentes à Inteligência Artificial, à Proteção de Dados, à Regulação e à Ética.

Caitlin Mulholland
Coordenadora da Graduação
em Direito da PUC-Rio

Introdução[1]

A interação contínua entre diversos aparelhos, sensores e pessoas altera a forma como agimos comunicativamente e tomamos decisões nas esferas pública e privada. Cada vez mais as informações que circulam não serão colocadas na Rede tão somente por pessoas, mas por Coisas e algoritmos[2] dotados de inteligência artificial que trocam dados e informações entre si, formando um espaço de conexões de rede e de informações cada vez mais automatizado.

Com isso, observamos 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 considerações éticas importantes tendo em vista os impactos progressivamente maiores da comunicação e da decisão algorítmica/computacional na sociedade.

A Internet das Coisas (*Internet of Things* — IoT) é a expressão que busca designar todo o conjunto de novos serviços e dispositivos que reúnem ao menos três pontos elementares: conectividade, uso de sensores e capacidade computacional de processamento e de armazenamento de dados. O que todas as definições de IoT têm em comum é que elas se concentram em como computadores, sensores e objetos (artefactos) interagem uns com os outros e processam as informações/dados em um contexto de hiperconectividade[3-4]. O atual cenário de hiperconectividade é, portanto, baseado na estreita

relação entre seres humanos, objetos físicos, sensores, algoritmos, *Big Data*, Inteligência Artificial (computacional)[5], *cloud computing*, entre outros elementos.

O termo hiperconectividade foi cunhado inicialmente para descrever o estado de disponibilidade dos indivíduos para se comunicar a qualquer momento. Esse termo possui alguns desdobramentos importantes[6]. 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 dados (*always recording*)[7]. 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[8-9]. Há, neste contexto, um fluxo contínuo de informações e uma 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* (tecnologias vestíveis) disponíveis no mercado e as várias opções de sensores utilizados no setor agrícola e nas indústrias[10] cada vez mais automatizadas com componentes de IoT e de Inteligência Artificial (em inglês, *Artificial Intelligence* — AI), fenômeno que vem sendo denominado de "Indústria 4.0".

Todos os dias, "coisas" se conectam à internet com capacidade para compartilhar, processar, armazenar e analisar um volume enorme de dados[11]. Quanto maior o número de dispositivos conectados, mais dados são produzidos[12]. Esta 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[13] que podem ser explorados para se obterem informações[14-15].

A primeira propriedade envolvendo *Big Data* consiste no volume crescente de dados[16]. Pesquisa recente da Cisco[17] estima que, nos próximos anos, a medida em gigabytes será superada e o cálculo da quantidade de dados será feito na ordem zettabyte e até mesmo em yottabyte[18].

Outra propriedade envolve a alta velocidade[19] 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[20].

O conceito[21] de *Big Data*[22] pode implicar ainda, juntamente com o conceito de *Data Science*[23], a capacidade de transformar dados brutos em 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[24].

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[25].

A combinação entre objetos inteligentes e *Big Data* poderá alterar significativamente a maneira como vivemos. Algumas pesquisas[26] 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 em 2025[27].

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, cada vez mais inteligentes e autônomos 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, devemos estar atentos aos riscos que podem trazer para a privacidade e a segurança dos usuários. Recentemente, testemunhamos o primeiro acidente fatal envolvendo um piloto automático de carro da empresa Tesla[28].

Presenciamos, ainda, o carro autônomo do Uber ultrapassar o sinal vermelho em São Francisco[29] e em 2018 atropelando e matando uma mulher nos EUA[30]; o algoritmo de reconhecimento facial do Registro de Motores de Massachusetts equivocadamente etiquetar alguém como um criminoso e revogar sua carteira de motorista[31]; o perfil robótico Tay, da empresa Microsoft, criado para interagir com técnica de *machine learning*[32] no Twitter, virando um bot de ofensas racistas e propagador de discurso de ódio em menos de 24 horas[33]; e a Arábia Saudita como o primeiro país do mundo a conceder cidadania a um robô[34], uma máquina (nomeada Sophia) dotada de inteligência artificial que ficou famosa no mundo com um vídeo[35] no qual dizia que iria destruir a humanidade[36].

Nas palavras de Marco Aurélio Castro[37]: "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 regularem juridicamente as novas Coisas inteligentes, capazes de imitar o comportamento humano e de outras máquinas, aprender com os próprios erros e demonstrar curiosidade, possuindo alto poder de investigação e processamento de informações, além de serem tão criativos e determinados quanto os humanos na resolução de desafios e na busca dos seus propósitos[38].

Diante desse cenário e na carência de regulação adequada pelo Direito, estamos vivenciando uma autorregulação do próprio mercado e uma regulação realizada muitas vezes através do *design* dessas novas tecnologias, o que denomino nesta obra de "tecnorregulação"[39]. A tecnologia está avançando mais rápido do que nossa habilidade de garantir a tutela[40] dos direitos individuais e coletivos.

Neste contexto, é crucial debatermos as noções de privacidade, segurança 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 e de Inteligência Artificial.

A nossa interação com as Coisas[41] tende a ser cada vez mais intensa. A governança dos dados e a compreensão e a regulação da agência dos diferentes actantes[42] humanos e não humanos neste cenário hiperconectado são fundamentais. 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, por 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. Exploraremos todas essas questões a partir de agora.

---

1 Algumas ideias desenvolvidas nesta obra constam do livro *A Internet das Coisas* (FGV, 2018), do mesmo autor, e são aqui retomadas, em especial, na introdução e no primeiro capítulo pela sua importância para o desenvolvimento dos argumentos e itens seguintes.

2 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.

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

4 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). Disponível em:

http://poetas.it.cesar.org.br/index.php/POETAS.IT:Sobre. Acesso em: 27 mar. 2017.

5 Comumente chamada de Inteligência Artificial (IA ou, da sigla em inglês, AI).

6 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.

7 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.

8 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.

9 Cf. FREDETTE *et al.*, 2012.

10 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.

11 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 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 definition: The General 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.

12 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 nem sequer possui acesso à internet e está excluída de todo este processo.

13 "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 tenham 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 de *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; 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.

14 LANE, Julia (Org.). *Privacy, Big Data and the public good*: frameworks for engagement. Cambridge: Cambridge University Press, 2014.

15 *"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.

16 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.

17 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.

18 Gigabyte é uma unidade de medida de informação que equivale a 1.000.000.000 bytes; zettabyte é uma unidade de informação que corresponde a 1.000.000.000.000.000.000.000 (10^{21}) bytes; e yottabyte é uma unidade de medida de informação que equivale a 10^{24} bytes.

19 Cf. RIJMENAM, op. cit., ago. 2015.

20 Cf. RIJMENAM, op. cit., ago. 2015. 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.

21 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 software, 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*".

22 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, José 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.

23 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 tornando-se 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.

24 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.

25 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.

26 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.

27 ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. *The Internet of Things*: an overview. Understanding the issues and challenges of a more connected world. ISOC, 2015, p. 1 e 4. Disponível em: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf. Acesso em: 30 mar. 2017.

28 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.

29 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.

30 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.

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

32 *"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.; DE VRIES, K. (Eds.) *Privacy, due process and the computational turn*: philosophers of law meet philosophers of technology. Abingdon: Routledge, 2013 p. 41-64.

33 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.

34 O termo "robô" advém da palavra checa *robota*, que significa servo ou trabalhador forçado. Portanto, é interessante notar que, na gênese do termo, há uma forte vinculação da ideia de robô como um servo moderno da humanidade. Apesar de a 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 programas de computador e algoritmos. A palavra robô pode se referir tanto a robôs físicos quanto a agentes virtuais de software, mas os últimos geralmente são chamados de *bots* (diminutivo de *robots*), também conhecidos na internet como *bots* ou *web robots*, consistindo geralmente em uma aplicação de software voltada a simular ações humanas repetidas vezes de maneira padrão. Aqui, especificamente, nos importam mais o conteúdo e o poder de agência/influência do que a forma de manifestação.

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

36 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.

37 CASTRO, Marco Aurélio. *Personalidade jurídica do robô e sua efetividade*. Salvador: 2009.

38 Vale ressaltar, apenas para fins de esclarecimentos conceituais, que nem toda inteligência artificial é humanoide e nem todas as coisas (digitais, conectadas ou analógicas) são inteligentes.

39 Termo cunhado pelo jus-filósofo italiano Ugo Pagallo.

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

41 Nesta obra, são compreendidos coisas e artefatos técnicos não somente como objetos físicos, materiais, mas qualquer engenho/ferramenta/utensílio construído para um determinado fim. Esse conceito engloba, portanto, desde exemplos de robôs físicos até algoritmos de programação.

42 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.

1. A Internet das Coisas: hiperconectividade, interação e Inteligência Artificial

A expressão IoT (sigla derivada do inglês, *Internet of Things*) é utilizada para designar a conectividade e interação entre vários tipos de objetos do dia a dia, sensíveis à internet[43]. 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[44]. 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[45].

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 meio da interconexão de coisas (físicas e virtuais) com base nas tecnologias de informação e comunicação interoperáveis existentes e em constante evolução[46].

A discussão sobre objetos conectados está presente desde os primórdios das tecnologias de informação[47]. 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"[48-49].

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"[50] 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)[51-52].

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[53], 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 os 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[54].

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 no rol de coisas que possivelmente se contrapõem à *Internet das Coisas úteis*, termo difundido pelo blog de tecnologia *MeioBit*[55].

Para fazer essa distinção de acordo com o potencial de utilidade, a *TrendWatching*[56], 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[57], 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.

Podemos citar como exemplo o *egg minder*[58], 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 dispositivo caro, com configurações complexas e baterias que precisam ser recarregadas constantemente[59]. 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?"*[60]:

> *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*[61].

Em complemento, sob o ponto de vista dos consumidores, aduzem Estéfano Veraszto *et al.*[62]:

> 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[63]. Segundo 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[64].

Esse problema é acentuado pela rápida perda de interesse nas "coisas inúteis". Pesquisas[65] 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[66], contribuindo para o já mencionado *e-waste*[67].

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 a segurança e privacidade[68]. 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 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*)[69-70].

A Federal Trade Commission dos Estados Unidos demonstrou preocupações com a segurança do ecossistema de IoT[71]. Por conta

disso, questionou o Department of Commerce recentemente sobre o assunto[72]. A Federal Trade Commission estima que cerca de dez mil habitantes podem gerar 150 milhões de *data points*[73] diariamente[74]. Os dispositivos captam as informações, enviam para a central e depois compilam os dados de acordo com as preferências do usuário[75].

Não se tem, hoje, clareza do tratamento dispensado aos dados[76]. Aspectos sobre a coleta, o compartilhamento e o potencial uso deles por terceiros ainda são desconhecidos pelos consumidores. Isso tem potencial de abalar — e, em certo sentido, já abala[77] — a confiança dos usuários nos produtos conectados[78].

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 uma série de ataques DDoS[79-80], 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 *smartwatches*, sacrificando a usabilidade só pela novidade. Essa técnica publicitária massiva que convence o consumidor a adquirir os mais diversos objetos acaba, segundo alguns autores, nos transformando em escravos da tecnologia[81].

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[82]:

> 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 uma vilã extremamente bem-sucedida.
>
> 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[83].

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[84]. Portanto, para que seja considerada uma invenção

stricto sensu, não basta ser uma criação do intelecto; é necessário que haja uma solução nova para um problema técnico existente[85].

O título jurídico pelo qual se protege uma invenção, assegurando ao seu titular uma relação de domínio ou propriedade[86], 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[87].

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"[88].

Nem toda invenção é considerada nova[89] — mesmo que para seu mentor o seja — por já poder estar acessível ao público. Ainda que se trate de novidade por 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[90].

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[91].

Entretanto, para o cumprimento desses requisitos, a maior dificuldade que se encontra é a própria definição da utilidade ou caráter industrial da invenção[92], 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"[93]. 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 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[94].

Vale, ainda, conferir os ensinamentos de Bercovitz[95], 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 úteis as forças naturais para a satisfação das necessidades humanas"[96].

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[97]. 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 inúteis[98]. 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 para nos manter sob constante vigilância por conta dos objetos que adquirimos[99-100].

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[101]:

> 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.[102]

Por outra perspectiva, as pesquisadoras Jenny Judge e Julia Powles destacam os lados negativos das invenções relacionadas à Internet das Coisas[103]:

> 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[104].

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[105]:

> 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[106].

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"[107].

Sobre esse aspecto, vale citar Estéfano Veraszto que examina, em seu estudo[108] "Tecnologia: Buscando uma definição para o conceito", as diferentes concepções e correntes acerca da tecnologia[109]. O autor explica no bojo deste 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[110]:

> 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 de 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 ideias 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.

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[111]. Segundo Galimberti[112]:

> 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.

Esse cenário de cultura hiperconectada e IoT vem sendo associado ao conceito de Web 3.0, possuindo em suas manifestações um forte

componente de tecnologia inovadora e relacionado a uma nova Era da Internet.

O termo *Web 3.0*[113] foi criado pelo jornalista John Markoff, do *New York Times*[114], 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"[115].

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, motivo; fim, escopo"[116-117-118]. 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"*[119].

Encontramos também uma definição dentro do âmbito jurídico relacionado ao Direito de Propriedade, diferenciando os conceitos de "coisa" e "bem". Parte considerável da doutrina[120] entende que "coisa" constitui um gênero, enquanto "bem" constitui espécie. Essa diferenciação foi adotada pelo Código Civil de 2002[121]. Os "bens", no direito civil, possuem classificação bem definida, vide artigos 79 a 103 do Código Civil[122].

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 coisa seria gênero, outras vezes seria espécie, e em algumas ocasiões existe 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"[123].

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 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[124].

É possível afirmar que a relação entre a IoT e a inteligência artificial será cada vez maior, merecendo uma explicação mais aprofundada sobre esse conceito. A inteligência artificial é um subcampo da informática. Seu objetivo é habilitar o desenvolvimento de computadores que sejam capazes de emular a inteligência humana ao realizar determinadas tarefas. O pesquisador de Stanford, John McCarthy, cunhou o termo em 1956 (durante a Conferência de Dartmouth), considerando que um programa de computador poderia ser considerado AI se fosse capaz de fazer algo que normalmente atrelamos à inteligência de seres humanos. A forma como se realiza a tarefa não é o problema segundo esta concepção, importa apenas ser capaz de fazê-la. Na concepção de outros teóricos, requer-se simplesmente que o trabalho seja realizado, não importando se o cálculo se relaciona de fato com o pensamento humano. Outras concepções estão no meio destas duas concepções, usando o raciocínio humano como modelo que pode informar e inspirar, mas não restritos à ideia de imitação dos humanos.

A tecnologia capaz verdadeiramente de simular o raciocínio humano se moldando a diferentes situações é denominada de “AI forte” (em inglês, *strong AI*), ou “AI geral” (em inglês, *Artificial*

General Intelligence). Os sistemas de AI projetados para tarefas específicas e predeterminadas são geralmente denominados de "AI limitada" (em inglês, *narrow AI*) ou "AI fraca".

É importante ressaltar, no entanto, que 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. Porém, 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.

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 e ferramentas mais inteligentes e focada no indivíduo. Especialistas acreditam que as utilidades da Web 3.0 poderão nos proporcionar uma espécie de assistente pessoal[125], que aprenderá cada vez mais sobre nós à medida que navegamos.

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[126]. 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[127]. 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[128].

A Web 3.0[129], 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 integrados, nos quais é possível usar apenas uma conta para utilizar variados serviços[130].

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)[131]. 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 Qualcomm não faz distinção nenhuma. Já a Cisco acredita

que a IoT é um estágio de transição para que possamos alcançar a IoE[132].

Definições e previsões sobre as próximas Webs também já estão sendo realizadas. Alguns estudiosos apontam que a Web 4.0 ou 5.0 será uma Web simbiótica[133], 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 Webs são assumidamente vagas, visto que o termo 2.0 até hoje é alvo de críticas[134] 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 e da inteligência computacional, exploraremos, a partir de agora, as regulações existentes e as possibilidades regulatórias futuras para esse cenário, bem como as estratégias e novas ferramentas de proteção da privacidade. Esse balanço inicial nos permitirá aprofundar as problemáticas envolvendo o norteamento ético e a tutela dos dados e das Coisas inteligentes no capítulo final.

43 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.

44 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.

45 *Id., ibid.*

46 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.

47 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.

48 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.

49 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.

50 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.

51 "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 registrar os dados sobre cada uma das coisas. A identificação por radiofrequência RFID oferece esta funcionalidade. Segundo, o registro 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 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.

52 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 as mudanças no ambiente dos aparelhos equipados.

53 "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, 2015).

54 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.

55 Confira-se a página disponível em: http://meiobit.com. Acesso em: 29 mar. 2017.

56 Cf. INTERNET OF caring things. *TrendWatching*, abr. 2014. Disponível em: http://trendwatching.com/trends/Internet-of-caring-things. Acesso em: 31 jan. 2017.

57 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.

58 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.

59 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.

60 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.

61 Tradução livre do autor: "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".

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 HOWER, Mike. As "Internet of things" grows, so do E-waste concerns. *Sustainable Brands*, 29 dez. 2014. Disponível em: www.sustainablebrands.com/news_and_views/waste_not/mike_hower/Internet_things%E2%80%99_grows_so_do_e-waste_concerns. Acesso em: 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.

64 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.

65 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.

66 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.

67 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.

68 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.

69 MAGRANI, Eduardo. *Democracia conectada*: a internet como ferramenta de engajamento político-democrático. Curitiba: Juruá, 2014.

70 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.

71 FEDERAL TRADE COMISSION. *Internet of Things*: privacy & security in a connected world. FTC Staff Report, 2015.

72 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.

73 "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".)

74 FEDERAL TRADE COMISSION, 2015.

75 FISHER, 2016b.

76 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.

77 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, 2015; 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.

78 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.

79 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-zumbi, entre outros métodos.

80 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.

81 JUDGE, 2015.

82 *Id., ibid.*

83 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".*

84 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, 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).

85 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.

86 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, 1982, 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".

87 CORRÊA, 2014, p. 64.

88 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.

89 Sobre o conceito de novidade, veja-se PHILPOTT, Jeremy. Patents. *In*: PHILPOTT, Jeremy; JOLLY, Adam. (Eds.). *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"*.

90 MAGRANI *et al.*, 2014.

91 *Id., ibid.*

92 PHILPOTT, 2004, 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)"*.

93 BARBOSA, Denis Borges. *Uma introdução à propriedade industrial*. 2. ed. rev. e atual. Rio de Janeiro: Lumen Juris, 2003, p. 319.

94 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.

95 MAGRANI *et al.*, 2014.

96 *Id., ibid.*

97 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.

98 CROUAN, 2016.

99 *Id., ibid.*

100 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.

101 GREENGARD, Samuel. *The Internet of Things*. Cambridge: The MIT Press, 2015, p. 188-189.

102 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".*

103 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.

104 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".*

105 JUDGE; POWLES, 2015, grifos do autor.

106 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 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".*

107 Cf. CZAJKOWSKI JR., Sérgio *apud* KARASINSKI, 2013.

108 VERASZTO, 2008.

109 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, autoevolutiva, 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 consequências 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 independentemente do contexto cultural, político, social ou econômico do local onde foi gerado. Isso dá a ideia que mesma tecnologia não tem seu uso modificado se inserida em outro contexto". O 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 técnica, 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, 2008).

110 VERASZTO, 2008.

111 Disponível em: http://filosofia.uol.com.br/o-humano-na-idade-da-tecnica/. Acesso em: 28 mar. 2017.

112 GALIMBERTI, Umberto. *The human being in the age of technique*. Unisinos, São Leopoldo 2015.

113 RAY, Kate. Web 3.0. *Vimeo*, maio 2010. Disponível em: https://vimeo.com/11529540. Acesso em: 27 mar. 2017.

114 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.

115 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.

116 Disponível em: https://www.priberam.com/dlpo/Objeto. Acesso em: 27 mar. 2017.

117 Disponível em: https://www.priberam.com/dlpo/objecto. Acesso em: 27 mar. 2017.

118 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.

119 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, contabilizados como coisas".

120 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. 28. ed. Rio de Janeiro: Forense, 2016.

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

122 "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, 2005.

123 Disponível em: https://www.boletimjuridico.com.br/doutrina/texto.asp?id=2478. Acesso em: 27 mar. 2017.

124 AGHAEI; NEMATBAKHSH; FARSANI, 2012, p. 6.

125 "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 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). O texto foi traduzido para o português por Fabiano Caruso e está disponível em: www.mail-archive.com/bib_virtual@ibict.br/msg01199.html. Acesso em: 27 mar. 2017.

126 SHANNON, Victoria. A 'more revolutionary' web. *The New York Times*, mai. 2006. Disponível em: www.nytimes.com/2006/05/23/technology/23iht-Web.html. Acesso em: 28 mar. 2017.

127 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 *et seq*.

128 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.

129 Ver vídeo ilustrativo sobre Web 3.0. Disponível em: www.youtube.com/watch?v=F_nbUizGeEY. Acesso em: 28 mar. 2017.

130 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.

131 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.

132 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.

133 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.

134 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.

2. 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) e inteligência artificial 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 a esse novo cenário.

Em especial, com relação à privacidade[135], os dispositivos da IoT, ao coletarem uma quantidade imensa de dados referentes a incontáveis aspectos da vida dos usuários, os coloca em um novo patamar de risco[136]. Sobretudo porque a lei brasileira de proteção de dados pessoais (Lei nº 13.709/18) ainda é recente, tendo sido

sancionada em 14 de agosto de 2018, após anos de discussão, e entrará em vigor apenas em 2020[137].

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 inter-relacionados, 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 Rodotà, como sendo "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular"[138].

Com relação ao conceito de proteção de dados pessoais[139], 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 o leque de garantias fundamentais que se encontram no ordenamento brasileiro[140]. Danilo Doneda, em relatório elaborado para a Escola Nacional de Defesa do Consumidor, pontua[141]:

> 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, mantêm 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[142] 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[143], a dignidade da pessoa humana é algo intrínseco a cada ser humano, que — por sua condição de humanidade — se torna merecedor do respeito e da consideração do Estado e dos outros seres humanos. Ainda segundo Sarlet, quando se fala em direito à dignidade, se está, em verdade, 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[144].

Segundo Maria Celina Bodin[145], 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[146]. 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 socioculturais 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"[147].

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 distinguem 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 em níveis diversos, respectivamente, sujeito e objeto.

Segundo o próprio Sarlet[148]:

> "[...] 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[149] 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 exercer sobre a vida em sociedade e a importância dos seus efeitos, inclusive sobre a esfera pública[150].

Por conta da quantidade de atores, artefatos e temas envolvidos, e do potencial surgimento de Coisas tão inteligentes quanto o ser humano ou até mais, com os avanços da inteligência artificial, a Internet das Coisas exigirá uma nova governança[151], 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[152]. Por isso, privacidade e segurança são tidas como duas das questões mais importantes da IoT[153].

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"[154].

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 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[155].

Enquanto não há legislação específica tratando da IoT e de Inteligência Artificial (AI), é preciso analisar, em primeiro lugar, os diplomas vigentes que podem ter aplicação neste setor[156] — sobretudo o CDC, o Marco Civil da Internet e a Lei nº 13.709/18, a Lei Geral de Proteção de Dados (LGPD). Veremos, a partir de agora, portanto, as regulações existentes e aplicáveis, dispostas em ordem cronológica.

---

135 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.

136 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.

137 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", que ainda não havia sido introduzida na legislação brasileira.

138 RODOTÀ, Stefano. *A vida na sociedade da 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.

139 Dados pessoais são todos aqueles que podem identificar uma pessoa como — números, características pessoais, qualificação pessoal, dados genéticos etc. *Dados sensíveis* são informações que podem ser utilizadas de forma discriminatória e, portanto, carecem de proteção especial, 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.

140 Vide: RODOTÀ (2008) e DONEDA (2006).

141 BRASIL, 2010, p. 39.

142 BRASIL, 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.

143 SARLET, Ingo Wolfgang. *Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988*. Porto Alegre: Livraria do Advogado, 2001, p. 50.

144 *Id.*, *ibid.*, p. 71.

145 Disponível em: https://dcivil1.blogspot.com.br/2015/09/o-principio-da-dignidade-da-pessoa.html. Acesso em: 27 mar. 2017.

146 CHAUI, Marilena. *Convite à filosofia*. 14. ed. São Paulo: Ática, 2010, p. 338.

147 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.

148 SARLET, Ingo Wolfgang. *Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988*. 4. ed. Porto Alegre: Livraria do Advogado, 2006.

149 CASTRO, 2009.

150 Para isso, as correntes 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.

151 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.

152 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.

153 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.

154 PRESCOTT, 2015.

155 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.

156 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., ao C.D.C. e à L.G.P.D., além do C.C. e da C.F. em função de relevância ser mais abrangente que os demais diplomas de menor escopo.

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*, a ação governamental capaz de proteger o consumidor garantindo "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 respeito da "educação e divulgação sobre o consumo adequado dos produtos e serviços", o que terá grande aplicabilidade à 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 xeque 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[157]. 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[158]. 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[159].

Nas palavras de Bruno Miragem, ao dissertar sobre a Internet das Coisas e os riscos do que considera um admirável mundo novo[160]:

> 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 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 incentivar a corrida industrial por aperfeiçoamento dos dispositivos. No entanto, é de suma importância que a indústria faça o maior esforço técnico possível de enviá-los ao mercado como produtos adequados à utilização da coletividade, ou seja, somente após passarem 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[161].

Corroborando 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"[162]. 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[163]. 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[164].

> *The Bluetooth-connected doll is marketed as a "friend you can talk with" via its embedded microphone. But again, it's a two-way 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. Germany 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[165].

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[166].

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.[167]

É importante termos em mente que todas essas tecnologias atreladas à IoT possuem vulnerabilidades[168]. No entanto, considerando que esses dispositivos estão cada vez mais complexos e inteligentes (dotados de inteligência artificial), 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[169].

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 (ou Alexa), capaz de programar diferentes tarefas, além de executar audiobooks e música, através do comando de voz. O dispositivo se comunica com o usuário atendendo aos seus comandos, assim como ocorre com Smart TVs.

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 tem capacidade de gravar vozes permanentemente, de modo que uma função específica e inerente ao seu funcionamento pode acabar 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 este produto com vulnerabilidades, porém, se isto ocorrer após a introdução do mesmo no mercado, o CDC prevê, no art. 10, parágrafo 1º, que o fato deve ser imediatamente comunicado às autoridades.

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 têm o dever de reparar o dano e/ou até mesmo indenizar o consumidor.

Exemplo de mau funcionamento ou defeito de produto com tecnologia IoT é o Nest Thermostat, um termostato inteligente da Amazon, que promete 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[170] 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[171], 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 à sua relação com a 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 de forma abusiva, há uma resposta direta do CDC. O artigo 6º, inciso IV, determina como direito básico a proteção do consumidor contra "publicidade enganosa e abusiva". 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[172].

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 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[173].

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.[174] Tal desequilíbrio de poder faz com que os consumidores se tornem hipervulneráveis e 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 IoT e Inteligência Artificial (AI) —, seus atuais dispositivos possuem aplicação direta à IoT e AI, conforme visto até aqui.

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 do CDC, 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".

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.

---

157 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.

158 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).

159 ZANATTA, 2017.

160 Disponível em: http://www.conjur.com.br/2017-mar-29/garantias-consumo-Internet-coisas-riscos-admiravel-mundo. Acesso em: 27 mar. 2017.

161 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.

162 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.

163 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.

164 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.

165 Tradução livre do autor: 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. 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.

166 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.

167 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.

168 Disponível em: http://www.bbc.com/news/world-europe-39002142. Acesso em: 27 mar. 2017.

169 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 possui o sistema Chaos Monkey, que expõe os engenheiros a falhas aleatórias e com muito mais frequência para incentivá-los a criar serviços mais resilientes.

170 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.

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

172 BRASIL, 2010, p. 59 *et seq*.

173 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.

174 ESTRADA, 2016, p. 42.

2.2. A regulamentação do Marco Civil da Internet (MCI) e a IoT

O Marco Civil da Internet (Lei nº 12.965/2014 — MCI)[175], aprovado em 2014, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Antes da sua sanção, 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[176-177].

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 proposição do PL nº 84/99[178], 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. Conforme descrito na obra *Democracia conectada*, deste mesmo autor[179]:

> 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[180].

O MCI se pretendeu como a "Constituição da Internet" no Brasil e salvaguardou diversos princípios e direitos fundamentais. A proteção da privacidade, dos dados pessoais e da liberdade de expressão são expressamente previstas no Marco Civil da Internet representando um grande avanço face ao cenário anterior ao diploma, que levava a uma quantidade maior de abusos e violações de direitos[181]. Além disso, suas disposições são fundamentais para um ambiente saudável e seguro tanto para IoT quanto para AI, tendo em vista a necessidade, nesses cenários, de direitos como acessibilidade, segurança dos dados, privacidade, entre outros previstos no MCI.

Em primeiro lugar, em sintonia com o relatório da ONU[182] que definiu em 2011 o acesso à Rede como um direito humano, o artigo 7º do MCI[183] possui extrema importância pelo fato de considerar o acesso à internet como essencial ao exercício da cidadania. Além disso, o mesmo artigo assegura inúmeros direitos aos usuários da internet no Brasil e tutela expressamente a privacidade em suas mais diferentes facetas. Complementarmente, o direito à privacidade e à liberdade de expressão são previstos no MCI como condição para o pleno exercício do direito de acesso à internet (art. 8º)[184].

Garante-se, no MCI, 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". Preveem-se, ainda, o direito a informações claras e completas sobre 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).

A proteção aos dados pessoais é tratada de forma específica na Seção II da Lei, cabendo destacar o que prevê o artigo 10[185]:

> 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.
>
> § 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** [grifo nosso].

Sobre a guarda de registros de conexão, o art. 13, caput, do MCI prevê o dever de os provedores de conexão mantê-los em sigilo e segurança pelo prazo de um 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 seis 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[186]:

> 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[187] até o tratamento futuro das informações produzidas, é preciso que as empresas estejam atentas à criação de mecanismos que assegurem a proteção da privacidade e a segurança dos usuários.

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 e aplicações de inteligência artificial estão sujeitos à lei e limitados por ela. Porém, apesar de o MCI ter representado um avanço significativo ao conseguir uma regulação ampla da internet, com a garantia de direitos básicos dos usuários, não esgota a proteção do cidadão no mundo de IoT e de AI.

O MCI não esgota a tutela geral do cidadão 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[188].

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 “dado pessoal” (que foi posteriormente prevista no Decreto que regulamentou o MCI e na Lei Geral de Proteção de 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.

Vale destacar, ainda, que o modelo de consentimento do usuário como elemento central para a permissão do uso de seus dados pessoais (necessidade de “consentimento expresso, livre e informado

sobre o tratamento dos dados pessoais") 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 intitulado *"Terms of Service and Human Rights"*[189].

Ademais, ainda que esse modelo fosse eficazmente aplicado, no cenário de IoT e AI, 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 verdadeiramente informado para o tratamento de dados irá impor um desafio enorme na prática para que seja realmente eficaz.

Alguns dos aspectos não tratados pelo Marco Civil foram previstos em Decreto, uma vez que que a Lei nº 12.655 é de base em grande medida principiológica, contando, por vezes, com uma escassez de detalhes sobre sua implementação[190]. O Decreto nº 8771/2016 regulamenta o Marco Civil da Internet e prevê desde conceituações importantes como a definição de "dado pessoal" até procedimentos específicos para tratamento, guarda e proteção de dados por provedores de conexão e de aplicações.

O art. 13[191] do Decreto trata dos padrões de segurança que devem ser observados por tais provedores. Complementarmente, o Instituto de Defesa do Consumidor (Idec)[192] 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 e do cumprimento de normas já existentes, como o Marco Civil e a lei geral de proteção de dados pessoais; (ii) *atualizações e vulnerabilidade*[193], sendo necessário pensar em

formas de obrigar os fornecedores a promoverem atualizações de sistema, correções de vulnerabilidade dos produtos e garantia de 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.

Outro exemplo de importante situação não contemplada expressamente pelo MCI é o serviço de *clouds*, amplamente utilizado atualmente por dispositivos conectados. As nuvens são espaços regidos por uma rede global de servidores, que atuam fornecendo conteúdo ou serviços[194], nos quais os usuários e empresas 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 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 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 se aplicam 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.

Portanto, o desafio maior é quando o servidor se encontra em outro país ou quando não há sede em território nacional. Tal previsão 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.

A nova LGPD, descrita em maiores detalhes na seção seguinte, traz alguns esclarecimentos que podem dar resposta a este problema. A legislação é explícita no sentido de que mesmo os atos praticados por entidades (públicas ou privadas) sediadas em outros países estão sob a sua jurisdição quando o tratamento de dados é realizado no território nacional, conforme estabelece o art. 3º da lei[195].

Dessa forma, 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 garantir sozinho uma proteção plena diante deste novo mundo de dados que se abre com a IoT e a AI, considerando tanto seu potencial quanto seus riscos a direitos fundamentais.

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[196]:

> 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.

A tutela da segurança e da privacidade do usuário, na forma do CDC e do MCI, será complementada pela entrada em vigor da Lei Geral de Proteção de Dados. Tanto isso é verdade que o próprio MCI, no art. 3º, inciso III, dispõe que a disciplina do uso da internet no

Brasil tem como princípio a "proteção dos dados pessoais, na forma da lei", que irá se ocupar da privacidade e da proteção dos dados pessoais dos usuários de modo mais minucioso e aplicável aos ambientes online e offline, nos quais os dispositivos de IoT poderão atuar, colhendo dados e informações pessoais relevantes dos titulares. Nesse sentido, 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.

---

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

176 MAGRANI, 2014.

177 SOUZA, Carlos Affonso; FRANCISCO, Pedro; MACIEL, Marília. Marco Civil da Internet: uma questão de princípio. Cadernos Colaborativos FGV Direito Rio, 2011, p. 118.

178 Também conhecida como Lei Azeredo pelo fato de o congressista Eduardo Azeredo ter sido o relator da proposta. Para mais informações sobre esse PL e seu contexto, vide: MAGRANI, 2014.

179 MAGRANI, 2014.

180 *Id., ibid.*

181 FORTES, Vinicius Borges. *Os direitos de privacidade e a proteção de dados pessoais na internet*. Rio de Janeiro: Lumen Juris, 2016, p. 120.

182 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.

183 "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."

184 "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."

185 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 mar. 2017.

186 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.

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

188 PRADO, 2014.

189 VENTURINI, Jamila *et al*. *Terms of service and human rights*: an analysis of online platform contracts. Rio de Janeiro: Revan, 2016, p. 74.

190 LEMOS, Ronaldo; SOUZA, Carlos Affonso. *Marco Civil da Internet*: construção e aplicação. Juiz de Fora: Editar, 2016, p. 30.

191 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."

192 ZANATTA, 2017.

193 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".

194 Disponível em: https://azure.microsoft.com/pt-br/overview/what-is-the-cloud. Acesso em: 7 fev. 2016.

195 No seu artigo 3º, a lei assim dispõe: "Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional".

196 MIRAGEM, Bruno. A Internet das Coisas e os riscos do admirável mundo novo. *Conjur*. 2017.

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, consistia, em artigo de 1890, no direito de ser deixado só (*right to be alone*)[197], já se via a necessidade de tutelar a proteção de dados pessoais. Com o desenvolvimento social e tecnológico, diferentes facetas deste princípio surgiram[198] e novos conflitos e problemas eclodiram, como o debate sobre o direito de não tomar conhecimento sobre um dado pessoal[199], a discussão sobre biografias não autorizadas[200] e o difícil enquadramento da privacidade no atual mundo de dados[201] refletido na IoT e nas esferas públicas conectadas[202].

O direito à privacidade, esfera do direito à vida privada, está intimamente conectado à proteção da dignidade e personalidade humanas[203], e pode ser extraído do reconhecimento constitucional dado à intimidade, à vida privada[204] e à inviolabilidade de dados[205]. 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[206-207].

Conforme visto nos itens anteriores deste capítulo, a privacidade também recebeu proteção infraconstitucional no Brasil. O Código Civil protege diretamente a vida privada[208] 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. Daí a importância da LGPD, que veio preencher as lacunas da legislação e é aplicável a uma gama mais ampla de usos da internet.

Na nova sociedade da informação, a privacidade deve ser entendida de forma funcional, de modo a assegurar a um sujeito a possibilidade de "conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas"[209]. Neste exato sentido, Stefano Rodotà complementa, definindo sinteticamente a proteção da privacidade como "o direito de manter o controle sobre as próprias informações"[210].

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[211] —, mas também o de liberdade positiva — ou seja, liberdade como autonomia, liberdade enquanto possibilidade de direcionar seu próprio querer sem ser determinado por outros[212-213] —, ligada ao controle dos dados. Essa perspectiva 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"[214].

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[215]. Como destaca Danilo Doneda, "esta crescente importância traduz-se no fato de que uma considerável parcela das liberdades individuais hoje são concretamente exercidas através de estruturas nas quais a comunicação e a informação têm papel relevante"[216].

O desenvolvimento tecnológico permite a criação de perfis de comportamento que podem até se confundir com a própria pessoa[217]. Tais perfis, aliados à manipulação de dados colhidos, podem gerar sérios impactos na liberdade dos indivíduos. Conforme nos explica Doneda sobre a técnica de coleta de dados pessoais conhecida como *data mining*[218]:

> 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, por outro lado, problemas à proteção da privacidade. Para Stefano Rodotà, 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"[219-220]. As mudanças sociais e tecnológicas exigem uma proteção específica da privacidade e, em particular, dos dados pessoais. Nas palavras de Carlos Affonso Pereira[221]:

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, e havia a necessidade de se criarem instrumentos legais para lidar com as novas tecnologias[222]:

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 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 networked society[223].

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[224]. Seria o pontapé inicial de um longo processo de discussão popular a respeito do tema, culminando na atual LGPD.

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, destacam-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 Rousseff, à época) e da Alemanha (Angela Merkel)[225], os quais apresentaram à Assembleia Geral da ONU uma proposta com regras para proteger o direito à privacidade na era digital[226].

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[227]. Já na Europa, todos os países, com exceção da Bielorrússia, possuem leis de proteção de dados pessoais[228]. 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[229].

No Brasil, o esboço do primeiro PL foi levado a debate público através do blog[230] 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 4.060/2012[231].

Durante os anos que se seguiram, diversos congressos e seminários[232] 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 nº 330/2013[233], nº 181/2014[234] e nº 131/2014[235], 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 Federal[236]. Em 2015, estes três projetos foram apensados e tramitariam em conjunto a partir de então.

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[237]. 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[238], além de dar sugestões sem se ater ao texto preexistente. O debate foi frutífero e contou com relevante participação dos cidadãos, tendo sido contabilizados 1.800 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[239].

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[240]. 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.

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 4.060/2012.

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 5.276/2016) foi proposto em 2016 pelo Poder Executivo.

É de salientar que o Anteprojeto nº 5.276/2016 foi recebido com urgência pela Câmara dos Deputados e, posteriormente, foi apensado ao PL nº 4.060/2012. Com esta unificação, ambos os

projetos passaram a tramitar pelo rito prioritário, o que significa que as Comissões teriam, em princípio, dez sessões para deliberar sobre eles. Em decisão de 24/08/2016, o Presidente da Câmara dos Deputados determinou a criação de uma Comissão Especial encarregada de discutir o PL nº 4.060/2012.

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 representou grande avanço nas questões de políticas digitais, inserindo esta pauta no cenário político brasileiro. 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.

A partir daí a tramitação na Comissão Especial perduraria por mais quase dois anos até ocorrer alguma movimentação substantiva. Durante esse período o PL veria reiterados pedidos de prorrogação de prazos e de realização de audiências públicas, muitas delas realizadas em diversas ocasiões e com vários atores da sociedade civil. Em 22 de maio de 2018, o deputado Orlando Silva, líder do PCdoB/SP e relator do projeto, encaminharia à Presidência da Câmara requerimento de urgência nos termos do art. 155 do Regimento Interno da Câmara dos Deputados. Dois dias depois, seu relatório seria publicado recomendando a aprovação do PL 4.060/12 e dos seus apensados, os PLs 5.276/16 e 6.291/16. O projeto iria ao plenário da Câmara, então, em 29 de maio de 2018, e, em Sessão Deliberativa Extraordinária, seria aprovado e encaminhado ao Senado Federal.

No Senado Federal, o PL 4.060/12 (e seus apensados) receberia nova numeração, tornando-se PLC (Projeto de Lei da Câmara) nº 53/2018. Lá receberia ainda os Projetos de Lei do Senado nº 330/2013, 131/2014 e 181/2014, tramitando em conjunto naquela casa. Sua passagem pelo Senado seria muito mais breve, com pouco mais de dois meses entre o início da tramitação, em 1º de junho de 2018, e a sanção presidencial com veto parcial, em 15 de agosto de 2018.

A questão do veto presidencial é importante, pois retirou do texto legal um componente crucial para a execução dos termos da nova lei. Os artigos 55 a 59 do PLC nº 53/18, vetados pelo Presidente, criavam e davam poderes e dotação orçamentária à Autoridade Nacional de Proteção de Dados. Esta seria uma entidade autárquica em regime especial vinculada ao Ministério da Justiça, ou seja, estaria sob regime semelhante ao das agências reguladoras. Com o veto do artigo que a criaria, fica a cargo da Presidência da República a iniciativa de nova lei para criá-la. Isto é de suma importância, pois diversos mecanismos de proteção de dados instituídos pela lei dependem da ação dessa autoridade. Conforme explicam Teffé e Mangeth[241]:

> Sua autonomia e independência são, sem dúvidas, essenciais para a efetividade das proteções dispostas para a privacidade e os dados pessoais. Como a Autoridade deve ter entre suas funções a possibilidade de monitorar o próprio Estado, ela deve se encontrar em posição que lhe permita atuar sem intervenções indevidas.
>
> [...]
>
> Dispõe o referido PL que a Autoridade terá como atribuições, por exemplo, zelar pela proteção dos dados pessoais; estimular a adoção de padrões técnicos bem como de serviços e produtos que facilitem o exercício de controle pelos titulares sobre seus dados pessoais; fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação; promover na população o conhecimento

> das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; promover ações de cooperação com autoridades de proteção de dados pessoais de outros países; dispor sobre as formas de publicidade das operações de tratamento de dados pessoais; solicitar às entidades do poder público, que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado; e realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o poder público.

A necessidade de uma lei geral que assegure a proteção de dados pessoais se aprofunda no cenário da Internet das Coisas[242]. Como pontua Stefano Rodotà, 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"[243]. 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"[244].

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[245], 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”[246].

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[247]. Neste sentido, a aprovação do PLC nº 53/2018 e sua conversão na Lei nº 13.709/18, a Lei Geral de Proteção de Dados, indica um passo positivo e necessário diante do cenário de IoT, além de representar o ponto culminante de todo o processo descrito anteriormente de discussão democrática e participativa da regulação brasileira de privacidade e tratamento dos dados pessoais.

Exploraremos a fundo no tópico seguinte as previsões regulatórias específicas contidas na 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[248].

---

197 WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890.

198 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.

199 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, 2012, p. 1-11.

200 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.

201 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: 7 fev. 2016.

202 MAGRANI, 2014.

203 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*. São Paulo: Revista dos Tribunais, 2012, p. 390.

204 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".

205 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".

206 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".

207 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.

208 "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."

209 RODOTÀ, 2008, p. 92.

210 *Id., ibid.*

211 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 de Carlos Nelson Coutinho. 2. ed. Rio de Janeiro: Ediouro, 1997, p. 48-49.

212 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, 1997, p. 51).

213 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.

214 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.

215 DONEDA, 2006, p. 153.

216 *Id., ibid.*, p. 153-154.

217 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, 2006, p. 173).

218 DONEDA, 2006, p. 176.

219 RODOTÀ, 2008, p. 95.

220 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.

221 SOUZA, Carlos Affonso. 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 guinada da *produção normativa* para que não se tutele a privacidade negativamente, mas positivamente, premiando, sobretudo, práticas que

assegurem o tão desejado controle de informações por parte dos usuários da internet" (BIONI, 2014, p. 80).

222 DONEDA; MENDES, 2014, p. 19.

223 Tradução livre do autor: "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 exigirão cada vez mais a criação de novos instrumentos de proteção de dados no Brasil para lidar com os riscos para a privacidade individual apresentada, por exemplo, pelo onipresente processamento de dados, a Internet de Coisas, on-line procurando e a Web 2.0. A actual revisão da directiva europeia e o Livro Branco sobre a privacidade digital, divulgados pelo governo dos Estados Unidos, ambos no ano de 2012, indicam a necessidade de criar novos instrumentos jurídicos em matéria de privacidade e 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 desenvolver, a fim de garantir direitos fundamentais e segurança jurídica em uma sociedade de redes".

224 Disponível em: https://economia.uol.com.br/ultimas-noticias/infomoney/2011/06/15/ministerio-da-justica-quer-lei-sobre-privacidade-e-protecao-de-dados-pessoais.jhtm.

225 Sobre o tema, v. BIONI, 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.

226 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: 7 fev. 2017.

227 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: 7 fev. 2017.

228 *Id., ibid.*

229 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.

230 Disponível em: http://pensando.mj.gov.br/dadospessoais2011. Acesso em: 28 fev. 2017.

231 Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066&ord=1. Acesso em: 27 mar. 2017.

232 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).

233 Disponível em: http://www25.senado.leg.br/Web/atividade/materias/-/materia/113947. Acesso em: 27 mar. 2017.

234 Disponível em: http://www25.senado.leg.br/Web/atividade/materias/-/materia/117736. Acesso em: 27 mar. 2017.

235 Disponível em: http://www25.senado.leg.br/Web/atividade/materias/-/materia/116969. Acesso em: 27 mar. 2017.

236 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.

237 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.

238 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.

239 Twitter: @dadospessoais; Facebook: https://www.facebook.com/Debate-P%C3%BAblico-Prote%C3%A7%C3%A3o-de-Dados-Pessoais-170882592934972/; Youtube: https://www.youtube.com/channel/UC4xogFvkir1ypVRKZeUsg5A. Acesso em: 27 mar. 2017.

240 Disponível em: http://pensando.mj.gov.br/dadospessoais/2015/04/protecao-de-dados-pessoais-pelo-mundo. Acesso em: 15 mar. 2017.

241 TEFFÉ, Chiara S.; MANGETH, Ana Lara. *Lei de Dados Pessoais precisa de uma autoridade independente*. ITS Rio. Disponível em: https://feed.itsrio.org/lei-de-dados-pessoais-precisa-de-uma-autoridade-independente-34137c7bbc64. Acesso em: 8 out. 2018.

242 "Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da internet, o acesso a dados sensíveis e, consequentemente, 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 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, 2012, p. 3).

243 RODOTÀ, 2008, p. 92.

244 *Id.*, *ibid*, p. 93.

245 *Id.*, *ibid.*

246 DONEDA, 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, 2000, p. 23).

247 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' 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"*.

248 Os Estados Unidos não possuem uma única lei federal abrangente que regula a coleta e o 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 de proteção 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.

2.4. Contrastes entre a regulação 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[249] e na Declaração Universal de Direitos Humanos[250]. 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 Federal de 1988. A interpretação da privacidade, contudo, vem mudando substancialmente nos últimos anos e esse direito ganhando novos contornos[251].

A tecnologia faz com que a esfera privada seja moldada de forma mais rica, contudo mais frágil e exposta a ameaças[252]. Por isso, tem-se a "necessidade do fortalecimento contínuo de sua proteção jurídica, da ampliação das fronteiras do direito à privacidade"[253]. No atual cenário, as mudanças sociais e tecnológicas exigem uma proteção específica da privacidade no Brasil e, em particular, dos dados pessoais[254].

O direito à privacidade configura um valor complexo[255], com diferentes significados e diversos aspectos que o caracterizam[256]. 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[257].

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 —, sob a ótica do segredo ou sigilo de determinadas informações e, por fim, sob a ótica do controle sobre informações e dados pessoais[258].

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[259]:

> 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[260].

Dentre os projetos de lei que tramitavam até então, inclusive o que deu origem à regulação atual, alguns buscaram inspiração na legislação europeia, o que se refletiu no texto final da lei e justifica, portanto, a comparação que faremos neste trabalho.

Conforme descrito no item anterior, entre os anos 2013 e 2014, foram propostos os PLs nº 330/2013, nº 181/2014 e nº 131/2014,

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 Federal[261]. Em 2015, estes três projetos foram apensados e tramitaram em conjunto até a aprovação do PLC nº 53/2018, atual Lei nº 13.709/18. Vimos também que o próprio PLC nº 53/2018 incluía os Projetos de Lei nº 4.060/2012 e 5.276/2016, sendo este fruto da discussão pública via plataforma digital empreendida pelo Ministério da Justiça.

O Projeto de Lei nº 5.276/2016, em especial, trazia importantes princípios para que a proteção da privacidade e dos dados pessoais fosse efetiva, prevendo, por exemplo, o princípio da finalidade[262], o princípio da adequação[263] e o princípio da necessidade[264]. Este PL sofreu forte influência da regulação europeia, guardando inúmeras semelhanças com o Regulamento Geral de Proteção de Dados (GDPR) — Regulamento (UE) 2016/679[265]. Muito do caráter protetivo desse PL se transferiu para a lei atual, que agora analisaremos em comparação com o GDPR.

O *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 proteção de dados para todos os indivíduos da União Europeia (EU). O GDPR entrou em vigor em 25 de maio de 2018, substituindo a diretiva de proteção de dados (Diretiva 95/46/CE) de 1995[266].

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[267]. 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 é executável desde 25 de maio de 2018 e, ao contrário de uma diretiva, 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[268].

Tanto o GDPR quando a LGPD, aplicáveis a entidades públicas e privadas que tratam dados pessoais, preveem diversos direitos aos titulares cujos dados são processados, disciplinam obrigações aos agentes de tratamento (controlador[269] e operador[270]); preveem a necessidade de se apontar um *data protection officer* (traduzido no Brasil como "encarregado[271]"); e estabelecem possíveis sanções.

Uma das similaridades que mais chama a atenção entre a Lei Geral de Proteção de Dados brasileira e o GDPR é quanto aos princípios. A Lei tem seus princípios dispostos no art. 6º, enquanto o GDPR os prevê em seu artigo 5º. Apesar de adotarem nomenclaturas distintas, os princípios são praticamente idênticos[272].

Os princípios garantidos pelo Regulamento Geral de Proteção de Dados (GDPR) exigem que cada controlador demonstre a conformidade com os princípios de proteção de dados[273].

> 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[274].

Dada a similitude da regulação europeia com a regulação brasileira, veremos a partir de agora em maiores detalhes como se manifesta cada um dos princípios previstos na nossa atual legislação.

O primeiro dos princípios garantidos pela Lei Geral de Proteção de Dados consiste no *princípio da finalidade* (art. 6º, I), exigindo que o destino a ser conferido aos dados deve ser informado previamente[275] aos usuários e que os dados colhidos só podem ser utilizados para fins legítimos, específicos e explícitos.

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)"[276]. 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 tratar-se de finalidades *devidamente informadas*; outros, como a CNI e a Febraban, 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[277]. No fim das contas, o texto aprovado da lei foi: "finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de

tratamento posterior de forma incompatível com essas finalidades" (art. 6º, I).

Pelo *princípio da adequação* (art. 6º, II), os dados coletados devem ser usados apenas na medida que forem necessários para atingir os objetivos anteriormente informados e de acordo com o contexto do tratamento.

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, 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[278]:

> 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 [atual] 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[279]. 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[280].

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 incorretas, cancelar aquelas registradas de forma indevida, suprimir as obsoletas ou impertinentes e, até mesmo, realizar acréscimos[281].

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 fiéis 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"[282].

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[283].

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 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), 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".

Apesar de já existirem riscos à segurança em computadores e redes tradicionais, eles são aumentados na IoT. Tais riscos são: "(1) permitir o acesso não autorizado e uso indevido de informações pessoais; (2) facilitar ataques a outros sistemas; e (3) criar riscos de segurança"[284]. Os princípios de segurança também devem ser aplicados quando da elaboração do design dos objetos, como se verá adiante[285]:

> *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.[286-287]

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[288].

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, IX)[289].

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 exemplifica Scott Peppet, empregadores podem avaliar os dados de candidatos a fim de decidir qual deles contratar[290].

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[291]:

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[292].

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[293] a estes dados, é possível fazer inferências sobre o estado físico, fisiológico e comportamental das pessoas. Confira-se[294]:

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. 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[295].

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[296].

Por fim, pelo princípio da *responsabilização e prestação de contas* (art. 6º, X), é requerido do agente que faz o tratamento dos dados que seja capaz de demonstrar a eficácia das medidas adotadas para o cumprimento das normas de proteção de dados pessoais.

Diante disto, chega em boa hora a nossa Lei Geral de Proteção de Dados[297] e é fundamental a sua aplicação efetiva por parte de empresas e da Administração Pública. Para tanto, é imperativo que a Presidência da República providencie o quanto antes a criação da Autoridade Nacional de Proteção de Dados. A existência de incontáveis dispositivos que utilizam a 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"[298-299].

Apesar de ainda ser discutível a necessidade de termos uma lei específica para tratar da IoT e da AI — a tecnologia ainda está em desenvolvimento e legislar sobre o tema agora seria prematuro sem um amplo debate ético na esfera pública — a aprovação de uma lei geral de proteção de dados pessoais já indica um passo positivo[300].

Com a lei não se objetiva frear inovações tecnológicas. Ela está, na verdade, em consonância com outras normas protetivas aos dados pessoais no cenário internacional[301]. 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 norteiam 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 constantemente"[302].

Nada obstante, o desenvolvimento da indústria relacionada à IoT sem a aprovação de uma lei de proteção de dados pessoais "é extremamente danosa"[303].

Diversas Organizações Não Governamentais juntaram-se para manifestar seu apoio à aprovação do PL nº 5276/2016, publicando uma carta aberta[304]. 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[305]. 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".

O espírito dos Projetos de Lei 5.276/2016 e 4.060/2012, que corriam em apenso até o início de 2018, foi transferido à Lei nº 13.709/18, a que deram origem. Ao mesmo tempo em que assegura direitos e garantias ao cidadão sobre seus dados, a Lei prevê regras e limites para que os setores privado e público utilizem esses dados, trazendo grande segurança jurídica e atendendo a demandas duplas[306]:

> 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.

Há outros pontos importantes de conexão, como a previsão sobre acesso facilitado às informações sobre o tratamento dos dados pessoais pelo titular. Pela lei, as informações devem ser disponibilizadas de forma clara, adequada e ostensiva sobre, dentre outros aspectos, a finalidade do tratamento, sua forma e duração (art. 9º). Similar a este regramento, o art. 12 do 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 transcritos a seguir:

> Lei 13.709/18, Art. 5º Para os fins desta Lei, considera-se: I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> GDPR, Artigo 4º 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 eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular;

As definições de dados pessoais sensíveis também são próximas. O GDPR prevê o conceito no art. 9º[307] e no preâmbulo (itens 10 e 51), ao passo que a lei brasileira o faz no art. 5º, inciso II[308] (dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou

político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural). Da mesma forma, o tratamento destinado a estes dados só pode ocorrer em situações específicas previstas em cada diploma[309].

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 o GDPR abrir a possibilidade para que Estados-Membros criem novas formas de punição.

Na Europa, assim como no Brasil, há limites claros de valor para a multa. 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 do 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.

A Lei nº 13.709/18 prevê como sanções (art. 52) — que podem ser aplicadas isolada ou cumulativamente — às pessoas jurídicas de direito privado que desrespeitarem as normas legais: (i) advertência, com indicação de prazo para adoção de medidas corretivas; (ii) multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 por infração; (iii) multa diária, observado o mesmo limite total; (iv) publicização da infração após devidamente apurada e confirmada a sua ocorrência; (v) bloqueio dos dados pessoais a que se refere a infração até a sua regularização; e (vi) eliminação dos dados pessoais a que se refere a infração. Os itens (i), (iv), (v) e (vi)

podem ser aplicados às entidades e aos órgãos públicos[310]. Sanções previstas em legislação específica não são substituídas pelas elencadas na Lei.

Com base no exposto, resta clara a forte influência da regulação europeia sobre a regulação no Brasil. Exploraremos, a seguir, algumas especificidades da normativa europeia tendo em vista tanto seus reflexos nas normas 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[311]. 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[312], o Tratado sobre o Funcionamento da União Europeia[313], o Tratado que estabelece uma Constituição para a Europa[314] e a Carta dos Direitos Fundamentais da União Europeia[315] asseguram esta proteção.

Na Europa, a *General Data Protection Regulation* (GDPR) (Regulamento UE nº 2016/679), aplicável desde 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[316].

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[317]. O GDPR foi proposto 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[318].

Dentre os agentes que devem observar os dispositivos do GDPR, estão as empresas que oferecem bens e serviços na União Europeia que lidem com dados pessoais de residentes na UE[319]. Tais empresas devem ser claras ao mostrar por que 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 da UE prevê direitos aos sujeitos cujos dados são processados; disciplina obrigações de controladores e operadores 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 o 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".

O GDPR, em seu Capítulo II, traz os princípios que devem ser observados pelos responsáveis pelo tratamento de dados pessoais[320]. 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[321]:

> **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 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, nº 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, nº 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 nº 1 e tem de poder comprová-lo ("responsabilidade").

O artigo 6º do 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 sejam compatíveis com a finalidade para a qual eles foram inicialmente recolhidos, devendo, para isso, ter em conta[322]:

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 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 9º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10;

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[323]. Há, entretanto, exceções a esta exclusão, previstas no item 2 do artigo 9º.

O 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 12.

De modo geral, quando os dados são recolhidos junto ao titular, o responsável pelo tratamento deve disponibilizar meios para própria identificação (identidade, contatos etc.), as finalidades do tratamento dos dados, o seu fundamento jurídico, os destinatários ou as categorias de destinatários dos dados pessoais e seus interesses legítimos, conforme disposto no art. 13 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. 13 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 ao titular, as regras aplicáveis são as previstas no art. 14. Similar a esta normatividade, temos, na Lei Geral de Proteção de Dados brasileira, o art. 9º 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. 17, 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 no GDPR, a saber[323][24]:

> 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 6º, nº 1, alínea a), ou do artigo 9º, nº 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, nº 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21, nº 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 8º, nº 1.

Além disso, há o direito à exclusão dos dados caso o responsável pelo tratamento os tenha tornado públicos, situação em que se deve observar o item 2 do art. 17[324][325]:

> 2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do nº 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 do 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 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. 20 prevê o direito de portabilidade dos dados, pelo qual o titular dos dados tem o direito de[326]:

> [...] 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 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[327]:

> 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[328]. Por isso, de grande aplicabilidade prática será a previsão do GDPR acerca da possibilidade de que o usuário não se sujeite a decisões tomadas exclusivamente com base em *profiling*.

Apesar dos diversos direitos previstos no 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. 23).

O Capítulo IV do 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 momento 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. 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[329-330]. Trata-se de conceito relativamente novo que está no centro dos debates sobre privacidade entre acadêmicos e legisladores[331].

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[332]:

> *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*[333].

Não há um modo de execução fixo pelo qual a proteção *by design* deve ser feita[334]. 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 no 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[335].

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[336].

No que tange à privacidade *by default*, confira-se[337]:

> *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*[338].

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[339], 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.

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[340], 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 9º, nº 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10; 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.

O 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[341-342].

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 operadores devem designar um responsável pela proteção de dados (*Data Protection Officers — DPO*), 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 do GDPR.

Tendo em vista a forte influência do GDPR na lei brasileira, bem como o impacto internacional que esta lei geral vem tendo desde a sua implementação obrigatória em maio de 2018, devemos estar atentos às especificidades deste marco legal em suas diferenças e similitudes com as regulações nacionais. A fim de que possamos aproveitar as oportunidades geradas pela IoT e pela A.I., é vital que busquemos um ambiente regulatório favorável.

Porém, mesmo após a aprovação da 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, a compreensão dessa legislação

torna-se cada vez mais difícil por conta do tecnicismo envolvido no debate e da maior complexidade das tecnologias atuais[343].

Além disso, a regulação jurídica que recai 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.

---

249 "Artigo 8º 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 econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros."

250 "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 à proteção da lei."

251 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, 2008, p. 23).

252 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, 2008, p. 92).

253 RODOTÀ, 2008, p. 95.

254 DONEDA; MENDES, 2014, p. 19; BIONI, 2014, p. 80.

255 POST, Robert C. Three concepts of privacy. *Georgetown Law Review*, v. 89, p. 2087, 2001.

256 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*. São Paulo: Editora Revista dos Tribunais, 2012, p. 393-394.

257 *Id., ibid.*, p. 394.

258 Sobre os diferentes conceitos de privacidade, v. LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2011, p. 52 *et seq*.

259 DONEDA, 2006, p. 14.

260 DONEDA, 2006, p. 1.

261 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.

262 "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."

263 "Art. 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."

264 "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."

265 Disponível em: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Acesso em: 27 mar. 2017.

266 Disponível em: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Acesso em: 27 mar. 2017.

267 *"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".*

268 Disponível em: http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018. Acesso em: 27 mar. 2017.

269 Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

270 Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

271 Pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador, os titulares e a autoridade nacional.

272 *"Article 5 of the GDPR requires that personal data shall be: 'a) processed lawfully, fairly and in a transparent manner in relation to individuals; 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.

273 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.

274 Disponível em: http://www.callcentermagazine.net/contact-centers/altitude-software-discute-novo-regulamento-da-protecao-dados. Acesso em: 27 mar. 2017.

275 Nota-se 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, 2015, p. 21-22).

276 BRASIL, 2010, p. 46.

277 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.

278 ZANATTA, 2017, p. 5.

279 FEDERAL TRADE COMISSION, 2015, p. 12.

280 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, 2015, p. 21).

281 BRASIL, 2010, p. 46.

282 *Id., ibid.*

283 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.

284 FEDERAL TRADE COMISSION, 2015, p. 10.

285 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.

286 FEDERAL TRADE COMISSION, 2015, p. 13.

287 Tradução livre do autor: "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 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".

288 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.

289 Vale mencionar que tanto o GDPR quanto a LGPD trazem à tona a discussão sobre "direito à explicação" que o titular dos dados teria no caso de decisão automatizada. Segundo o art. 20 da lei brasileira, o titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. O direito à explicação (*right to explanation*) possui o condão de auxiliar o titular dos dados no caso de tratamento automatizado possivelmente injusto e discriminatório realizado a partir dos seus dados pessoais. Esse direito tende a ganhar extrema relevância nos próximos anos, com o avanço das decisões algorítmicas e da Inteligência Artificial.

290 PEPPET, 2014.

291 Tradução livre do autor: "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, podem-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".

292 PEPPET, 2014, p. 121.

293 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 algorithm 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.

294 Tradução livre do autor: “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”.

295 PEPPET, 2014, p. 122-123.

296 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”.

297 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.

298 *Código de Defesa do Consumidor*, art. 6º, I.

299 ZANATTA, 2017, p. 4.

300 FEDERAL TRADE COMISSION, 2015, p. 49.

301 Neste sentido, para ZANATTA (2017, p. 12): “É importante lembrar que os princípios gerais do PL 5.276/15 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 5.276/15 não configura obstáculo à inovação, estando bastante alinhada com os desenvolvimentos jurídicos recentes”.

302 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.

303 ZANATTA, 2017, p. 5.

304 Disponível em: http://www.idec.org.br/pdf/carta-aberta-pl-dados-pessoais-jun2016.pdf.

305 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".

306 MENDES; DONEDA, p. 48.

307 "Artigo 9º *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."

308 "Art. 5º. Para os fins desta Lei, considera-se: II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural."

309 Confiram-se os art. 11 a 13 da Lei nº 13.709/2018 e o art. 9º do GDPR.

310 Os incisos VII, VIII e IX inicialmente previstos na Lei foram vetados na fase de sanção presidencial. Esse artigo sofreu alteração, ainda, da Medida Provisória nº 869/2018, pendente de aprovação até o momento de elaboração da presente obra, sujeita a sanção presidencial, com a seguinte redação: "Art. 52: X – suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. § 2o O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. § 3o O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. § 5o O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. § 6o As sanções previstas nos incisos X,

XI e XII do caput deste artigo serão aplicadas: I – somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e II – em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. § 7o Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo".

311 FORTES, 2016, p. 153-154.

312 "Artigo 39 Em conformidade com o artigo 16 do Tratado sobre o Funcionamento da União Europeia e em derrogação do nº 2 do mesmo artigo, o Conselho adopta uma decisão que estabeleça as normas relativas à proteção 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."

313 "Artigo 16 (ex-artigo 286 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 circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes."

314 "Artigo I-51 *Protecção de dados pessoais* 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. A lei ou lei-quadro europeia estabelece 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 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."

315 "Capítulo II, Artigo 8º *Protecção de dados pessoais* 1. Todas as pessoas têm direito à proteção 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."

316 PROMONTORY. EU GDPR: A Primer. 19 fev. 2016. Disponível em: http://www.promontory.com/News.aspx?id=4127. Acesso em: 7 mar. 2017.

317 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.

318 PROMONTORY. EU GDPR: Summary of Key Provisions. Disponível em: http://www.promontory.com/uploadedFiles/Articles/Insights/151221_GDPR_compromise_A4.pdf. Acesso em: 8 mar. 2017.

319 O art. 3º(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 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".

320 Uma comparação entre os princípios previstos na legislação europeia e na legislação brasileira foi feito no tópico II.

321 Disponível em: https://www.eugdpr.org. Acesso em: 27 mar. 2017.

322 Disponível em: https://www.eugdpr.org. Acesso em: 27 mar. 2017.

323 Confira-se 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".

324 Disponível em: https://www.eugdpr.org. Acesso em: 27 mar. 2017.

325 Disponível em: https://www.eugdpr.org. Acesso em: 27 mar. 2017.

326 Disponível em: https://www.eugdpr.org. Acesso em: 27 mar. 2017.

327 DONEDA, 2006, p. 173.

328 *Id., ibid.*, p. 174.

329 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: Springer, 2014, p. 446.

330 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.

331 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.

332 CAVOUKIAN, Ann. Privacy by design. *IEEE Technology and Society Magazine*, winter 2012, p. 19.

333 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".

334 KLITOU, 2014, p. 266.

335 HOEPMAN, 2014, p. 452-457.

336 CAVOUKIAN, 2012, p. 19.

337 Tradução livre do autor: "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".

338 Disponível em: http://www.eudataprotectionregulation.com/data-protection-design-by-default. Acesso em: 17 mar. 2017.

339 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".

340 "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 nº 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."

341 Sobre o tema, confira-se o Capítulo VI do GDPR, que trata sobre autoridades de controle independentes.

342 Os itens 127 e 128 do preâmbulo trazem uma explicação sobre o assunto. Confira-se: "(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".

343 ZIEGELDORF, Jan; MORCHON, Oscar; WHERLE Klaus. Privacy in the Internet of Things: threats and challenges. *Security and Communications*, volume 7, issue 12, p. 2728-2742, 2014.

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)[344] 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.

---

344 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.

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?'."
(Kurt Vonnegut, *Cama de gato*, 1963)

Quando se discutem ética e avanço tecnológico uma das discussões mais tradicionais que se costuma trazer *a priori* envolve o embate entre as visões contrastantes do utilitarismo/consequencialismo[345] 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[346]. 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 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[347].

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 US$ 11 por veículo, aplicável a 12,5 milhões de carros e caminhões leves, chegando a um total de US$ 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 US$ 49,5 milhões para a sociedade, de acordo com o quadro a seguir[348]:

QUADRO 1.

BENEFITS

Savings	180 burn deaths, 180 serious burn injuries, 2.100 burned vehicles
Unit cost	$200.000 per death, $67.000 per injury, $700 per vehicle
Total benefit	(180 x $200.000) + (180 x $67.000) + (2.100 x $700) = **$49.5 million**
COST	
Sales	11 million cars, 1.5 million light trucks
Unit cost	$11 per car, $11 per truck
Total cost	12.5 million X $11 = **$137.5 million**

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, esta realizou um *recall* voluntário, antes que a NHTSA lançasse a ordem formal de *recall*[349].

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 a 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.

A visão utilitarista clássica, preconizada por Jeremy Bentham em 1781[350], é caracterizada pelo que muitos autores chamam de consequencialismo. Deste modo, busca encontrar justificação nas consequências das ações, e não em máximas absolutas[351]. A visão utilitarista clássica[352] 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[353]. 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"[354]. 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"*[355]. Essa visão utilitarista clássica resiste, portanto, à ideia de que a justiça moral depende de qualquer outra coisa que não seja suas consequências[356].

Segundo John Rawls[357], 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[358].

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[359]:

> 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 consequência 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[360]. [grifo nosso]

No mesmo sentido, segundo o professor de Harvard Michael Sandel[361], 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.[362]

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 Mill[363] e Posner[364], 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 bem-estar da sociedade, independentemente de o agente saber antecipadamente se essas condições serão — ou não — cumpridas.[365-366]

Esse problema se intensifica no cenário de Internet das Coisas, que traz mais imprevisibilidade para a equação e torna ainda mais difícil, quiçá 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[367].

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[368].

A deontologia enquadra-se no domínio das teorias morais que orientam e avaliam o que devemos fazer e, de modo diverso das teorias utilitaristas, julgam a moralidade das escolhas individualmente, por um parâmetro não orientado pelos resultados[369].

O primeiro grande filósofo a definir princípios deontológicos foi Immanuel Kant[370], fundador alemão da filosofia crítica do século 18 e talvez o maior representante dos ideais iluministas[371]. 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[372]. Nas palavras do 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![373]

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 19 e 20 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[374].

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.[375] Ele viu a 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[376]:

> (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, independentemente do sopesamento das consequências[377]. 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 à 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 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 contraintuitivo 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 consequências 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[378].

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[379]. Portanto, parte do problema da utilização desta tese decorre da vagueza do conceito de utilidade e 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[380].

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*[381] e *deep learning*[382], nos deparamos com invenções que não permitem, muitas vezes, a previsão de consequências.

Conforme nos ensina o pesquisador holandês Peter Kroes, ainda que um designer possa antecipar diferentes consequências não planejadas e não determinadas, ele não pode evitar que todas essas consequências negativas surjam. A partir desse ponto de vista, o desenvolvimento tecnológico sempre tem um caráter experimental: algumas consequências sociais de uma determinada tecnologia só emergem quando esta é implementada[383].

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 preestabelecidas, 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[384]:

> *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*[385].

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[386].

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 esta visão, a ênfase internacional hoje na proteção dos direitos humanos — e, portanto, no dever de não os violar — 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[387]. 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 direito de escolher a não existência de futuras gerações em função da existência da atual, ou mesmo de as colocar em risco[388].

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[389].

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[390], 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[391].

As questões de esfera pública de Habermas estão ligadas à evolução tecnossocial e à concepção kantiana de uso público da razão[392], entendida como um fator essencial para se atingir o processo de esclarecimento — *Aufklärung*. Esse processo, para Habermas, conforme veremos, depende da ação comunicativa na

esfera pública, refletido a partir do debate racional-dialógico capaz de atingir o consenso e o verdadeiro conhecimento[393].

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.

---

345 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 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.

346 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.

347 BINDER, Denis. The increasing application of criminal law to disasters and tragedies. *Natural Resources & Environment*, v. 30, n. 3, 2016.

348 BAURA, Gail. *Engineering ethics:* an industrial perspective. Cambridge: Academic

Press, 2006, p. 39-50.

349 ROSSOW, Mark P. *Ethics:* an alternative account of the Ford Pinto case, 2015.

350 BENTHAM, Jeremy. *Os pensadores*. São Paulo: Abril Cultural, 1979.

351 *Id., ibid.*

352 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. Acesso em: 20 set. 2017.

353 MILL, John Stuart. *O utilitarismo*. São Paulo: Iluminuras, 2000.

354 COSTA, C. Razões para o utilitarismo. *Ethic@*. Florianópolis: UFSC, v.1, n. 2, p. 155-174, 2002.

355 Tradução livre do autor: "A maior felicidade para o maior número de pessoas".

356 SANCHEZ VASQUEZ, Adolfo. *Ética*. 14. ed. Rio de Janeiro: Civilizacao Brasileira, 1993.

357 RAWLS, John. *A theory of justice*. Harvard, 1971.

358 SANDEL, Michael. *Justiça*: o que é fazer a coisa certa? Rio de Janeiro: Civilização Brasileira, 2009.

359 RAWLS, 1971.

360 RAWLS, John. *Uma teoria da justiça*. Trad. Almiro Pisetta e Lenita Maria Rimoli Esteves. 2. ed. São Paulo: Martins Fontes, 2002, p. 25.

361 SANDEL, 2009.

362 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 cinco pessoas seriam salvas, mesmo às custas da morte de uma pessoa, o resultado final seria um bem maior.

363 MILL, 2000.

364 POSNER, Richard. *Economic Analysis of Law*. Chicago, 2014.

365 FRANKENA, William K. *Ética*. Rio de Janeiro: Zahar, 1969. 143p.

366 Disponível em: https://plato.stanford.edu/entries/consequentialism/#WhaGooHedVsPluCon. Acesso em: 10 jan. 2018.

367 Disponível em: https://plato.stanford.edu/entries/consequentialism/#WhaGooHedVsPluCon. Acesso em: 10 jan. 2018.

368 Disponível em: https://pt.wikipedia.org/wiki/Dilema_do_bonde. Acesso em: 29 abr. 2017.

369 Disponível em: https://plato.stanford.edu/entries/ethics-deontological/#AgeCenDeoThe. Acesso em: 29 abr. 2017.

370 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 consequências 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. First section: transition from the common rational knowledge of morals to the philosophical, groundwork of the metaphysic of morals. *In*: ABBOTT, Thomas Kingsmill (Ed.). *Fundamental principles of the metaphysic of morals*. 10.ed. 1975. Disponível em: https://en.wikipedia.org/wiki/Deontological_ethics#cite_note-transition-11.

371 Segundo Fraga: O Iluminismo pode ser definido como um movimento filosófico surgido ao longo do século 18 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 ideia 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.

372 KANT, Immanuel (1784). *Beantwortung der Frage: Was ist Aufklärung*.

373 KANT, 1784.

374 Disponível em: https://esbocosfilosoficos.com/2014/03/14/a-visao-politica-de-thomas-hobbes. Acesso em: 29 abr. 2017.

375 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 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/.

376 KANT, Immanuel. *Fundamentação da Metafísica dos Costumes* (Grundlegung zur Metaphysik der Sitten, 1785). Trad. Paulo Quintela. Lisboa: Edições 70, 2008.

377 Disponível em: https://plato.stanford.edu/entries/ethics-deontological/#AgeCenDeoThe. Acesso em: 29 abr. 2017.

378 Disponível em: http://www.newworldencyclopedia.org/entry/Deontological_ethics. Acesso em: 29 abr. 2017.

379 Tradução livre do autor.

380 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.

381 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.

382 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 aprendizagem de máquinas que não são necessariamente inspiradas nos sistemas neurais humanos.

383 KROES, Peter *et al. A philosophy of technology:* from technical artefacts to

sociotechnical systems. San Rafael: Morgan & Claypool Publishers, 2011.

384 KROES, 2011.

385 Tradução livre do autor: “Isto se dá, em parte, também devido 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 a questões éticas das condições sobre as quais essas experiências seriam moralmente aceitáveis.

386 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.

387 Disponível em: https://www.britannica.com/topic/deontological-ethics. Acesso em: 29 abr. 2017.

388 JONAS, Hans. *O princípio responsabilidade*: ensaio de uma ética para a civilização tecnológica. Rio de Janeiro: Contraponto, 2015.

389 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.

390 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.

391 HABERMAS, Jürgen. *Between facts and norms*: contributions to a discourse theory of law and democracy. Cambridge: Polity Press, 1992.

392 KANT, Immanuel. *A paz perpétua e outros opúsculos*. Lisboa: Edições 70, 1784 (1992). HABERMAS, Jürgen. *The theory of communicative action*: reason and the rationalization of society. Vol. 2. Cambridge: Polity Press, 1986.

393 HABERMAS, 1992.

3.2. A esfera pública colonizada por algoritmos: artefatos tecnológicos (agentes não humanos) na esfera pública conectada

Conforme vimos anteriormente, é importante que busquemos, para os propósitos de regulação da IoT e da AI, a prevalência da perspectiva orientada pela proteção de direitos humanos. Este primeiro alicerce nos permite contornar os abusos advindos da perspectiva 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[394]. A partir disso, podemos pensar então qual a perspectiva ética mais adequada para atender aos procedimentos e às 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[395].

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[396]. 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[397].

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[398].

Conforme explicado previamente em trabalho do autor deste livro[399], a esfera pública de Habermas constitui uma zona de intercâmbio[400] entre o sistema, de um lado, e os espaços públicos e privados do mundo da vida, de outro. O sistema é caracterizado por Habermas como o mundo do trabalho, pautado pela lógica do dinheiro e do poder[401], como um mundo instrumental de ação estratégica, e não comunicativa, orientado pelo mercado e pela burocracia[402]. O mundo da vida, por sua vez, é descrito por Habermas como o mundo da interação entre pessoas, 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[403].

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 impacta destrutivamente a reprodução cultural, na integração social e na socialização, como componentes do mundo da vida[404].

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*[405], a possibilidade de se compreenderem 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 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, deve ser incluída 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 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[406].
>
> [...]
>
> 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[407].

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 nocivos sobre a democracia e freando o entusiasmo acerca do papel democrático da internet como esfera pública para as sociedades contemporâneas[408].

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, através de mecanismos de busca e redes sociais, 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*[409] — 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 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.

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 o 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 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 como 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[410], já atentava para a força da mídia tradicional e seu impacto para a democracia moderna neste sentido[411].

No entanto, muitas vezes as plataformas de internet não possuem transparência suficiente no recorte informacional e algorítmico 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[412]. 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 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[413].

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 sociopolítica com base nesses fatores[414].

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[415]. O autor Frank Pasquale faz uma crítica a essa situação, tratando os algoritmos de hoje como caixas-pretas e jogando luz sobre os efeitos disso em uma sociedade guiada em diversas áreas por dados e decisões algorítmicas[416].

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[417] e influenciam a opinião pública postando e replicando mensagens em larga escala. Muitos *bots*[418] (robôs)[419] têm replicado hashtags que ganham destaque com a massificação de postagens automatizadas de forma a sufocar debates espontâneos sobre um determinado tema.

A princípio, as contas automatizadas podem até contribuir positivamente em alguns aspectos da vida nas redes sociais. Os *chatbots*[420] (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[421].

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[422].

Corroborando essa tese, em uma pesquisa recente, a Diretoria de Análise de Políticas Públicas (DAPP) da FGV[423] identificou interferências ilegítimas no debate online através do uso de *bots*. Contas programadas para postagens massivas se converteram em

uma potencial ferramenta para a manipulação de debates nas redes sociais.[424]

> 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[425].
>
> [...]
>
> 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[426] 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[427].

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 de atrair usuários para links maliciosos que roubam dados pessoais, entre outros riscos[428].

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[429-430].

Segundo o estudo[431]:

> 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 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[432]:

> 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-robô 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[433].

O estudo do uso de robôs no período analisado[434] 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-robô 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 técnicos[435] (como *bots*) são mais do que o suficiente para jogar luz sobre uma ameaça real à qualidade do debate na esfera pública[436].

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 uma *chatbot* — um programa de Inteligência Artificial —, denominada 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 de 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: 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.

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[437]?

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 análise 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 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.

---

394 Impõe-se, portanto, um "dever ser" ético e moral não somente atrelado às finalidades, mas também a todo procedimento e gama de ações.

395 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 obra *Democracia conectada*), razão pela qual não nos aprofundaremos tanto nos conceitos básicos do autor ou justificaremos exaustivamente sua ligação com as esferas digitais.

396 Disponível em: https://plato.stanford.edu/entries/habermas. Acesso em: 28 nov. 2017.

397 Com a publicação em 1962 de sua habilitação, *Strukturwandel der Öffentlichkeit* (Transformação Estrutural da Esfera Pública, ed. Inglesa, 1989).

398 MAGRANI, 2014.

399 *Id.*, *ibid*.

400 "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, 2014).

401 Sistema econômico e poder político-administrativo.

402 HABERMAS, 1986; CALHOUN, Craig (Ed.). *Habermas and the public sphere*. Cambridge: The MIT Press, 1992, p. 1-51.

403 "As esferas públicas são o lugar por excelência para a deliberação política e autodeterminação democrática através de espaços públicos e privados. O sistema político, entendido como o aparato burocrático do Estado, cede lugar para que as deliberações políticas ocorram nas esferas públicas, visando à formação coletiva da vontade, à justificação de decisões previamente acertadas e ao surgimento de novas identidades. E através dos procedimentos democráticos e das suas pressuposições comunicativas, a

soberania popular é reinterpretada intersubjetivamente" (MAGRANI, 2014, p. 25).

404 Apesar de Habermas prever que não haja uma blindagem completa do mundo da vida da lógica sistêmica, acredita na capacidade de essa lógica ser anulada pela própria dinâmica do mundo da vida, pautado no agir comunicativo.

405 MAGRANI, 2014, p. 25.

406 *Id., ibid.*

407 MAGRANI, 2014.

408 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.

409 WU, Tim. *The master switch*: the rise and fall of information empires. New York: Vintage. 2011.

410 WIGGERSHAUS, Rolf *et al. The Frankfurt School*: its history, theories, and political significance. Cambridge: The MIT Press, 1995.

411 HABERMAS, 2003, p. 99.

412 MAGRANI, 2014.

413 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.

414 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.

415 PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

416 Recentemente, em Wisconsin, nos Estados Unidos, um juiz concedeu uma pena de prisão de seis anos levando em consideração não somente o registro criminal do réu, mas também sua pontuação na escala COMPAS (Correctional Offender Management Profiling for Alternative Sanctions). COMPAS é uma ferramenta algorítmica de que visa a 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 foi 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.

417 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.

418 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 predeterminadas. 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.

419 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.

420 Disiponível em: <https://medium.com/@tecnoequidade/especialistas-explicam-como-o-robô-pode-influenciar-o-debate-nas-redes-3a844f911849>. Acesso em: 29 abr. 2017.

421 Disponível em: http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-Web.

422 *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 da mostra 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.

423 Disponível em: http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf. Acesso em: 29 abr. 2017.

424 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.

425 Disponível em: http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf. Acesso em: 29 abr. 2017.

426 Os primeiros *bots* 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 desinformação para manipulação na esfera pública. Um *Twitter Bot* é uma conta controlada por um algoritmo ou script, normalmente utilizadas para realizar tarefas repetitivas, por exemplo, retuitar conteúdo contendo palavras-chave particulares e responder ou enviar mensagens diretas a novos seguidores. *Twitter Bots* mais complexos podem participar de conversas online e, em alguns casos, têm um comportamento muito parecido 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 frequentemente 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.

427 "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 a 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.

428 Sobre a existência hoje de um "exército" de perfis falsos, vide: http://www.bbc.com/portuguese/brasil-42172146. Acesso em: 14 mar. 2018.

429 Disponível em: http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf. Acesso em: 29 abr. 2017.

430 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 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; 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: 9 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.

431 *Id., ibid.*

432 Disponível em: http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf. Acesso em: 29 abr. 2017.

433 Disponível em: http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf. Acesso em: 29 abr. 2017.

434 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-robô 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.

435 Artefatos aqui devem ser compreendidos não somente como objetos físicos, materiais, mas qualquer engenho/ferramenta/utensílio construído para um determinado fim. Engloba-se nesse conceito, portanto, desde robôs físicos a algoritmos de computação.

436 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 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 a tradição ou dogma precisam ser expostos; e, como consequência, a verdade é alcançada por meio da busca ao consenso.

437 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.

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[438] e epistemológica[439] para se entenderem 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 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 preveem os próximos livros *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*[440].

Sobre as influências possíveis a partir da interação com essas novas Coisas, uma interessante e recente pesquisa[441] 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 executar instruções e até mesmo conversar com o usuário em linguagem natural)[442], 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[443].

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[444].

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[445]:

> *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*[446].

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, 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"[447].

O pensamento entendido como pós-humanista vem buscando compreender e tecer novas concepções sobre o distanciamento da ideia que temos de condição 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[448], 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[449].

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[450], 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, relaciona-se com a nossa subjugação ao pensamento tecnológico da atualidade, o pensamento cibernético[451].

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 autoprogramação) 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 assegurarem 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 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 têm 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[452]. Vale dizer, adota-se uma postura contra o pensamento do período iluminista. Como se sabe, na modernidade, buscava-se a "autoemancipação de uma humanidade razoável"[453], 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[454] não foi capaz de impedir as horríveis guerras e os campos de concentração[455]. Para Latour, o conceito de modernidade ou de racionalidade humana não teria qualquer conteúdo preciso[456]. 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 micropoderes de governamentalidade[457].

Com base nisso, Latour desenvolve junto a outros teóricos a chamada "Teoria Ator-Rede", segundo a qual humanos e não humanos interagem entre si e influenciam-se mutuamente[458]. 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[459]. Essa perspectiva acaba com os privilégios dos homens e põe fim às hierarquias, já que, ontologicamente, todos os seres estão no mesmo nível[460-461].

Segundo Gustavo Amaral[462], 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 os seres como relevante. “O que Sartre disse dos humanos — que a existência deles precede a essência — deve ser dito de todos os actantes”[463].

Uma das bases do pensamento de Latour se encontra na ideia do princípio da simetria[464], utilizado de forma generalizada para alcançar igualdade formal entre conceitos que foram historicamente definidos a partir de dicotomias, como humano/não humano[465]. 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”[466].

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[467]. Adicione-se a isto o fato de que a ação para Latour depende da associação de actantes[468], 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”[469].

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 características de um tornam-se atributos de outro e vice-versa. Nas palavras de Latour[470]:

> 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: devem-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[471-472]. 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[473], o que traz consequências até quanto à responsabilidade por atos que envolvam humanos e não humanos[474]:

> 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 de 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[475].

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 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[476].

Portanto, a definição de actante é obtida por meio do papel que ele possui na rede e os efeitos que gera nela, podendo ser desde pessoas, animais, coisas, objetos até instituições, o que terá implicações no debate sobre responsabilidade e 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[477].

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[478]. 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 à 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, criando nas pessoas a ideia de pertencimento e similaridade e, por fim, estabilizando nossa vida através de rituais repetidos no dia a dia.

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[479]. 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 reconhece a necessidade de uma nova lente teórica, crítica à perspectiva dualista. O novo materialismo, nesse contexto, desvencilha-se de concepções deterministas que consideram a matéria como algo ontologicamente predeterminado, para estabelecer uma teoria que valoriza a construção de sentido contínua e dinâmica, a partir de uma abordagem mais ampla do conceito de causalidade[480]. 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"[481]:

> *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*[482].

Nesse sentido, essa perspectiva buscou afastar-se do pensamento dual 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[483].

Segundo Nick Fox[484]:

> *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*[485].

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, ou seja, como algo que 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 elementos, que são sempre potenciais[486]. 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 intrarrelacionados.

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 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[487]. 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[488].

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 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[489].

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 de 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[490].

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[491].

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[492]. 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*]”[493].

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[494]. 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[495].

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[496]. Em complemento a 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 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"[497].

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[498]:

> 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 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"[499].

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 explicam 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[500]. 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 medeia a relação destes com outros não humanos[501].

Nesse sentido, destaca-se trecho do *Relatório sobre Ética e Algoritmos* da Algorithms Watch:

> *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*[502].

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 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[503].

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 tornar-se políticos, não apenas por serem usados para intermediar conflitos entre atores políticos, mas principalmente porque essas ferramentas estão imbricadas na estrutura humana e social[504]. 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 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.

---

438 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.

439 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.

440 Disponível em: http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepWebwhitepaper1.pdf. Acesso em: 29 set. 2017.

441 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.

442 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.

443 Disponível em: http://www1.folha.uol.com.br/colunas/ronaldolemos/2017/11/1936624-como-falar-com-as-maquinas.shtml. Acesso em: 18 out. 2017.

444 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.

445 *Les mots et les choses* (The order of things, 1966).

446 Tradução livre do autor: "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 18, pode-se certamente apostar que o homem seria apagado, como um rosto desenhado na areia à beira do mar".

447 WEINBERG, Darin. Social constructionism. *In*: TURNER, Bryan S. (Ed.). *The new Blackwell companion to social theory*. Chichester, UK: Wiley-Blackwell, 2009, p. 281-299.

448 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.

449 Cf. HARAWAY, Donna. A cyborg manifesto: Science, technology and socialist-feminism in the late twentieth century. *In*: HARAWAY, Donna. *Simians, Cyborgs, and Women*. The Reinvention of Nature. Nova York: Routledge, 1991.

450 Cf. REGIS, Edward. *Great Mambo Chicken and the Transhuman Condition*: science slightly over the edge. Woburn: Perseus Books, 1990 *apud* RÜDIGER, 2007.

451 RÜDIGER, 2007.

452 LATOUR, Bruno. *Jamais fomos modernos*: ensaio de antropologia simétrica. Trad. Carlos Ireneu da Costa. São Paulo: Editora 34, 1994.

453 ROUANET, Sergio Paulo. *Mal-estar na modernidade*. São Paulo: Companhia das Letras, 1993, p. 97.

454 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 *et seq*.

455 FEENBERG, Andrew. Modernidade, tecnologia e formas de racionalidade. In: BEIRA, Eduardo (Org.). *Tecnologia, modernidade e democracia*. Lisboa: MIT Portugal/ IN+/Inovatec, 2015, p. 191 e 193.

456 CORREIO DO POVO. 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: 7 ago. 2017.

457 FOX, Nick J.; ALLDRED, Pam. New materialist social inquiry: designs, methods and the research-assemblage. *International Journal of Social Research Methodology*, v. 18, n. 4, p. 400, 2015.

458 Cf. LAW, John; LODGE, Peter. *Science for social scientists*. London: Macmillan Press, 1984.

459 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 *et seq*.

460 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.

461 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.

462 AMARAL, 2015, p. 106.

463 LATOUR, 1994.

464 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, 2015, p. 96-97.

465 AMARAL, 2015, p. 94.

466 LATOUR, 2001, p. 210

467 AMARAL, 2015, p. 105 e 108-109.

468 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.

469 LATOUR, 2001, p. 210.

470 *Id., ibid.*, p. 218-219.

471 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, 2001, p. 219).

472 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 uma organização semissocial 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 uma 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, 2001, p. 240).

473 Nas palavras do autor: “Uma vez que a palavra agente no caso dos não humanos é incomum, um termo melhor é actante, 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 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.

474 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, 1994, p. 34).

475 VERBEEK, Peter. *Moralizing technology*: understanding and designing the morality of things. Chicago: The University of Chicago Press, 2011.

476 *Id., ibid.*

477 LATOUR, 1994.

478 *"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"* (grifo nosso). LATOUR, 1994, p. 41. 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, 2001, p. 218).

479 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.

480 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.

481 Disponível em: https://newmaterialistscartographies.wikispaces.com/New+Materialism. Acesso em: 28 nov. 2017.

482 Tradução livre do autor: "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 criar o novo, um futuro desconhecido, que não é mais reconhecível em termos do presente. Na arte, essa análise poderia ser o estudo da matéria e do significado".

483 Disponível em: http://www.tandfonline.com/doi/full/10.1080/13645579.2014.921458. Acesso em: 19 set. 2017.

484 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.

485 Tradução livre do autor: “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”.

486 ARADAU, Claudia. Discourse/materiality. *In*: ARADAU, Claudia *et al. Critical security methods: new frameworks for analysis*. New York: Routledge, 2014, p. 57-84.

487 ARADAU, 2014.

488 LEMKE, Thomas. New materialisms: Foucault and the ‘government of things’. *Theory Culture & Society*, april 2014.

489 *Id., ibid.*

490 *Id., ibid.*

491 FERNÁNDEZ, Maria. *Posthumanism, new materialism and feminist media art*.

492 BARAD, Karen. *Meeting the universe halfway*: quantum physics and the entanglement of matter and meaning. Durham: Duke University Press, 2007.

493 *Id., ibid.*

494 PARIKKA; TIAINEN, 2010.

495 ARADAU, 2014.

496 LATOUR, B. *Reassembling the social*: an introduction to actor-network theory. Oxford: Oxford University Press, 2005.

497 JONAS, 2015.

498 SANTOS, Boaventura de Souza. *A nova Tese Onze*. 2018. Disponível em: http://outraspalavras.net/capa/boaventura-a-nova-tese-onze. Acesso em: 29 set. 2017.

499 LAW, J.; SINGLETON, V. *Performing technologies’ stories*: on social construtivism, performance, and performativity. Technology and Culture, 2000.

500 LATOUR, 1994.

501 LEMOS, André. *A comunicação das coisas*: Teoria Ator-Rede e cibercultura. São Paulo: Annablume, 2013.

502 Tradução livre do autor: “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”.

503 LATOUR, 2005.

504 BARRY, A. *Political Machines*: Governing a Technological Society. London: Athlone Press, 2001.

3.4. Ética das coisas e governança de algoritmos em artefatos e sistemas sociotécnicos

"By ratiocination, I mean computation."[505]
(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[506].

Em uma escala ainda maior, essa é a tese reforçada pelo escritor israelense Yuval Noah Harari[507] ao tratar da perda de liberdade humana e do que denomina de a nova religião dos dados[508]:

> *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 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*[509].
>
> *[...]*
>
> *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*[510].

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[511].

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[512]. 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[513].

A governança de algoritmos[514] 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[515]. 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 basear-se no interesse público. Já no caso da regulação governamental, foca-se em requisitos como o nível de transparência ou de qualidade do serviço[516].

Dentre os pontos de regulação, se encontram a transparência, a responsabilidade — que se liga às noções de justiça e devido processo — e as garantias técnicas, além do desenvolvimento de princípios éticos relativos ao uso de dados pessoais (*Big Data Ethics*). Destaque-se que os algoritmos estão trabalhando constantemente e enfrentam situações não previstas e sem precedentes com frequência, de modo que seu monitoramento deve ser constante[517].

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[518].

Segundo Relatório elaborado por grandes nomes do ramo de Ética Digital como Luciano Floridi e Wendell Wallach[519]:

> *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*[520].

Sobre esse problema, aprofundam o debate os pesquisadores do Oxford Internet Institute e Alan Turing Institute[521]:

> *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 data-driven 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 decision-making processes both accessible and comprehensible. The longstanding problem of interpretability in machine learning algorithms indicates the challenge of opacity in algorithms. [...] Transparency disclosures by data processors and controllers may prove crucial in the future to maintain a trusting relationship with data subjects*[522].

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[523].

A 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.

Na Europa, o GDPR (*General Data Protection Regulation*), mencionado anteriormente, 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[524]:

> *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*[525].

Pesquisadores da Universidade de Zurique[526] 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[527]. 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[528]. Se os dados são algo fundamental para os algoritmos, que são inertes até que pareados com bases de dados[529], 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[530]:

> *This is true for several tools already present in data protection 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*[531].

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:

> *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 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*.[532-533]

Já Lucas Introna[534], 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

metagovernança, 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 contêm 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[535]:

> *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'*[536].

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[537-538]:

> *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*[539].

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[540], o YouTube 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[541]. 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[542].

Esse ponto nos leva a discutir de maneira mais aprofundada a responsabilidade moral desses agentes (ou actantes) não humanos[543]. Para isso e 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"*[544].

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[545]:

> Conceber humanidade e tecnologia como polos 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, 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*[546].

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*[547], 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[548]. 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 aos papéis dos indivíduos e das instituições sociais em relação a eles e a seu uso[549].

Nas palavras de Kroes[550]:

> *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*[551].
>
> *[...]*
>
> *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*[552].
>
> *[...]*
>
> *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.*[553]

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 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[554]. 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[555]. 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[556].

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 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[557]. 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 impedirem consequências não premeditadas e também de responsabilização dos agentes em caso de dano, uma vez que a "ação tecnológica" refletida no sistema sociotécnico é uma soma de ações de actantes entrelaçados na Rede em uma intrarrelação[558].

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 os 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 têm processos operacionais predefinidos 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[559]. 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)[560].

Segundo M. C. Elish, da Universidade de Columbia[561]:

> *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 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*[562].

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[563].

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.

Colin Allen e Wendell Wallach[564] argumentam que, à medida que Coisas inteligentes como os robôs[565] possuem cada vez mais autonomia e assumem cada vez mais responsabilidade, eles devem ser programados com habilidades morais de decisão para nossa própria segurança[566].

Corroborando essa tese, Peter-Paul Verbeek[567], ao tratar da moralidade das Coisas, entende que: como as máquinas[568] operam com mais frequência 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, defendemos 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 3.2 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*, 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 em menos de 24 horas depois do início de seu funcionamento, em função da produção de resultados preocupantes[569].

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 antissemitas. 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 gorila a fotos de pessoas negras[570].

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[571].

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.*[572], isso não os exime da responsabilidade de 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 preestabelecidas 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[573], 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[574].

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[575] 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 monitorado o comportamento do *bot* de forma intensa nas primeiras 24 horas de seu lançamento, o que não se sabe se ocorreu[576].

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[577].

Outro caso[578] 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*[579].

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[580].

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[581-582]. Segundo relatório divulgado no Fórum Econômico Mundial de 2017[583]: "*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 precondições para a responsabilidade por danos. Contudo, como não se reconhece hoje a Inteligência Artificial como um sujeito de direito, ela não pode ser considerada individualmente responsável pelos potenciais danos que pode causar[584]. 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, ser responsável por qualquer ação gerada pela máquina. Esse raciocínio pauta-se pela noção de que uma ferramenta não possui vontade própria[585].

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"[586-587].

Há, ainda, a possibilidade encontrada no modelo cujo foco está na habilidade de os programadores ou usuários preverem o potencial de ocorrência desses delitos. 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[588] em face de um resultado que seria previsível[589].

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[590]. 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[591]. Por outro lado, o autor sustenta que a aplicação da disciplina da responsabilidade por imperícia, por sua vez, possui grande potencial[592]. Se encontraria, dessa forma, entre a responsabilidade objetiva (*strict liability*) e a negligência. O standard, nesse caso, deveria ser fixado pela comunidade profissional[593].

No entanto, enquanto o campo se desenvolve, para Cole, o 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[594].

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 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[595-596]. 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[597-598].

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[599].

Pelo fato do comportamento de uma AI não ser totalmente previsível e seu comportamento ser o resultado da interação entre diversos agentes humanos e não humanos que compõem o sistema sociotécnico e até mesmo de processos de *self-learning*, pode ser extremamente difícil encontrar o nexo causal[600] entre o dano gerado e a ação de um ser humano ou pessoa jurídica[601].

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[602].

Segundo sustentam os pesquisadores do Alan Turing e Oxford Internet Institute[603]:

> *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*[604].

Corroborando essa tese, segundo o recente relatório[605] da UNESCO sobre *robotics ethics*:

> *The rapid development of highly intelligent autonomous robots, then, is likely to challenge our current classification of beings according to their moral 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*[606].

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[607]. 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[608], inclusive no cenário regulatório, sem que se tenha definido 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[609], 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.

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[610].

Conforme se extrai da parte de responsabilidade do texto (9)[611], 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 no quadro a seguir, produzida no estudo da UNESCO[612], traz parâmetros importantes que nos ajudam a pensar sobre essas questões tentando identificar as diferentes agências envolvidas. Embora a estrutura proposta seja simples, sua implementação em termos de atribuição de responsabilidade e regulação do uso é complexa e desafiadora — para cientistas e engenheiros, decisores políticos e eticistas.

QUADRO 2.

DECISION BY ROBOT	HUMAN INVOLVEMENT	TECNOLOGY	RESPONSIBILITY	REGULATION
Made out of finite set of options, according to present strict **criteria**	Criteria implemented in a legal framework	Machine only: deterministic algorithms/robots	Robots' producer	Legal (standards, national or international legislation)
Out of a range of options, with room for flexibility, according to present **policy**	Decision delegated to robot	Machine only: AI-based algorithms, cognitive robots	Designer, manufacturer, seller, user	Codes of practice both for engineers and for users; precautionary principle
Decisions made through	Human controls	Ability for human to take control over	Human beings	Moral

human-machine **interaction**	robot's decisions	robot in cases where robot's actions can cause serious harm or death		

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[613].

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[614] a robôs inteligentes deve ser levada em consideração, tendo em vista o ganho de autonomia[615] das Coisas inteligentes[616]. Nesse sentido, conforme sustenta o professor da GeorgeTown University, David Vladeck[617]:

> *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*[618].

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[619].

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 arguir que ser pessoa é necessariamente ser-humano. Temos hoje o precedente inclusive de entidades empresariais enquadradas com status jurídico de pessoa[620]. 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[621], entre outras capacidades e habilidades. Nas palavras de Castro[622]:

> 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.

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 passo importante.

A nova proposta europeia reflete uma resposta prática mais célere para o problema mencionado anteriormente de "irresponsabilidade distribuída"[623], 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 existência de um único nexo causal que não pode ser identificado de forma direta, podemos atribuir 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 casos de dano, pode não ser suficiente para a atribuição justa de responsabilidade na era de IoT e de inteligência artificial forte[624].

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[625].

Vale destacar a parte de responsabilidade como consta na Resolução[626-627]:

> *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 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 fund, the limits of its liability in case of damage to property, the names and the functions of the contributors and all other relevant details;

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[628-629]*;*

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. Apesar de a nossa tecnologia ainda não ter desenvolvido robôs dotados de um nível de autonomia suficiente para substituir completamente o ser humano em tarefas complexas e que exigem alto grau de adaptação, haverá muito provavelmente um momento em que essa autonomia será possível e, quando esse momento chegar, deveremos ter mecanismos teóricos para implementar esse tipo de atribuição de responsabilidade, mas de forma a não provocar um efeito inibidor a inovações tecnológicas, nem gerar uma irresponsabilidade generalizada por parte de empresas, fabricantes e prestadores de serviço.

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[630]:

> *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*[631].

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 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 sociotécnica e suas esferas de controle e influência sobre as situações e sobre os demais agentes.

Porém, ainda estamos longe de obter um consenso razoável[632] 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[633] artificiais[634], com capacidade de tornarem-se AIs cada vez mais fortes (*strong AI*).

Certamente, as razões para justificar uma personalidade eletrônica ainda não estão aqui pelo fato de ainda não termos desenvolvido inteligências artificiais fortes (strong AIs). No entanto, como a inteligência computacional cresce exponencialmente, assim como seu nível de interação em nossas vidas cotidianas e na esfera pública conectada, com o ganho de novas etapas de autonomia, devemos inevitavelmente pensar em possibilidades de estabelecer novas

formas de prestação de contas e responsabilidade pelas ações da AI, incluindo a possibilidade de atribuir direitos, subjetividade ou até mesmo uma personalidade eletrônica no futuro próximo.

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.

---

505 Hobbes uses "ratiocination" to mean reasoning. In: SOBEL, Carolyn P. *et al. The cognitive sciences*: an interdisciplinary approach. Los Angeles: Sage, 2013. Disponível em: http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=3447&context=nclr. Acesso em: 29 set. 2017.

506 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.

507 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: "*ICTs 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 (infogs), 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.

508 Disponível em: https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c.

Acesso em 27 nov. 2017.

509 Tradução livre do autor: “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, veem 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”.

510 Tradução livre do autor: “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 frequência 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”.

511 SAURWEIN, Florian; JUST, Natascha; LATZER, Michael. Governance of algorithms: options and limitations. *Info*, v. 17, n. 6, p. 35-49, 2015.

512 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.

513 DONEDA, Danilo; ALMEIDA, Virgilio A. F. What is algorithm governance? *IEEE Internet Computing*, v. 20, p. 60, 2016.

514 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; JUST; LATZER, 2015, p. 38-43.

515 DONEDA; ALMEIDA, 2016, p. 61.

516 *Id. ibid.*, p. 62.

517 *Id. ibid.*

518 DONEDA; ALMEIDA, 2016, p. 60-62.

519 WALLACH, Wendell *et al. Artificial Intelligence for the common good: sustainable, inclusive and trustworthy*. 2017. Disponível em: https://weforum.ent.box.com/v/AI4Good?platform=hootsuite. Acesso em: 28 fev. 2017.

520 Tradução livre do autor: "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".

521 MITTELSTADT, Brent et al. The ethics of algorithms: Mapping the debate. *Big Data & Society*, Jul.-Dec. 2016.

522 Tradução livre do autor: "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 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, a 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".

523 Disponível em: http://www.businessinsider.com/algorithmic-bias-accountability-bill-passes-in-new-york-city-2017-12. Acesso em: 28 nov. 2017.

524 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.

525 Tradução livre do autor: "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".

526 SAURWEIN; JUST; LATZER, 2015, p. 37 *et seq*.

527 *Id. ibid.*

528 DONEDA; ALMEIDA, 2016, p. 61.

529 GILLESPIE, Tarleton. The Relevance of Algorithms. *In*: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo J.; FOOT, Kirsten A. (Eds.). *Media technologies:* essays on communication, materiality, and society. Cambridge: 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"*.

530 DONEDA; ALMEIDA, 2016.

531 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".

532 SAURWEIN; JUST; LATZER, 2015, p. 44.

533 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".

534 INTRONA, Lucas D. Algorithms, governance, and governmentality: on governing academic writing. *Science, Technology, & Human Values*, v. 41, n. 1, p. 17-49, 2016.

535 Tradução livre do autor: "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".

536 INTRONA, 2016.

537 Heurística é um método ou processo criado com o objetivo de encontrar soluções para um problema.

538 Tradução livre do autor: "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".

539 DIAKOPOULOS, 2015, p. 400.

540 *Id., ibid.,* p. 401.

541 DIAKOPOULOS, 2015, p. 398: *"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"*.

542 BOSTROM, Nick; YUDKOWSKY, Eliezer. A ética da inteligência artificial. *Fundamento: Revista de Pesquisa em Filosofia*, v. 1, n. 3, p. 202-203, 2011.

543 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 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" (KNIGHT, 2017).

544 VERBEEK, 2011.

545 LATOUR, 2001, p. 245.

546 *"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".* Disponível em: http://webfoundation.org/docs/2017/07/AI_Report_WF.pdf.

547 KROES, 2011, p. 1-2 e 5-7.

548 *Id., ibid.*, p. 1-2.

549 *Id., ibid.*, p. 1-2 e 11.

550 *Id., ibid.*, p. 1-2 e 5-7.

551 Tradução livre do autor: "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".

552 Tradução livre do autor: "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".

553 Tradução livre do autor: "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".

554 KROES, 2011, p. 7-13.

555 *Id., ibid.*, p. 9-10.

556 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).

557 KROES, 2011, p. 1-2 e 67.

558 Os conceitos de entrelaçamento (*entanglement*) e intra-ação encontram explicação aprofundada nas seções anteriores deste capítulo.

559 SARAIVA, Leonardo. *Sistema de análise de erros humanos na prevenção de acidentes aeronáuticos*, 2011.

560 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 perspectiva que enxerga não somente os aviões como artefatos técnicos isolados, mas pensando em soluções que envolvam o sistema sociotécnico de forma mais ampla. Disponível em: http://www.airport-technology.com/features/featureair-traffic-control-easy-target-hackers.

561 ELISH, M. *Moral crumple zones*: cautionary tales in human-robot interaction, 2016.

562 Tradução livre do autor: "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, que 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 ambiguidade 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".

563 Em sua definição habermasiana.

564 WALLACH, Wendell; ALLEN Colin. *Moral machines*: teaching robots right from wrong, Oxford: Oxford University Press, 2008.

565 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.

566 Em complemento, os pesquisadores da Delft University of Technology e da Eindhoven University of Technology sustentam que os valores que devem ser levados em consideração no desenvolvimento destas tecnologias são: saúde, segurança, sustentabilidade e privacidade.

567 VERBEEK, 2011.

568 *"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'."* Disponível em: https://perma.cc/EJ5M-YMCJ.

569 Disponível em: https://tecnoblog.net/193318/tay-robo-racista-microsoft. Acesso em: 27 set. 2017.

570 Disponível em: https://www.tecmundo.com.br/google-fotos/82458-polemica-sistema-google-fotos-identifica-pessoas-negras-gorilas.htm. Acesso em: 27 set. 2017.

571 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.

572 *Id., ibid.*

573 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.

574 DONEDA; ALMEIDA, 2016, p. 60.

575 WOLF, 2017.

576 *Id., ibid.*

577 WOLF, 2017.

578 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 intermedeia 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.

579 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.

580 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.

581 VLADECK, David C. Machines without principals: liability rules and artificial intelligence. *Washington Law Review*, vol. 89, n. 1, mar. 2014. p. 120-121.

582 CERKA, Paulius *et al*. Liability for damages caused by artificial intelligence. *Computer Law & Security Review*, vol. 31, n. 3, jun. 2015. p. 376-389.

583 Disponível em: https://weforum.ent.box.com/v/AI4Good?platform=hootsuite. Acesso em: 27 set. 2017.

584 CERKA, 2015.

585 *Id., ibid.*

586 O problema desta abordagem é que as Coisas começam a partir de agora a se treinarem 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 advêm 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". Disponível em: 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.

587 CERKA, 2015.

588 *US v. Andrews*, 75 F.3d at 552.

589 HALLEVY, Gabriel. The criminal liability of Artificial Intelligence entities: from science fiction to legal social control. *Akron Intellectual Property Journal*, vol. 4, 2010.

590 COLE, George S. Tort Liability for Artificial Intelligence and expert systems. *Computer/Law Journal*, vol. 10, n. 2, 1990.

591 *Id., ibid.*

592 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.

593 COLE, 1990.

594 COLE, 1990.

595 PAGALLO, Ugo. *The laws of robots*: crimes, contracts and torts. Dordrecht: Springer, 2013.

596 VLADECK, 2014.

597 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 "autoensinam"? 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?

598 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.

599 CERKA, 2015.

600 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.

601 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 consequência 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, 2009.

602 Disponível em: http://unesdoc.unesco.org/images/0025/002539/253952E.pdf. Acesso em: 27 set. 2017.

603 MITTELSTADT, Brent *et al.* The ethics of algorithms: Mapping the debate. *Big Data &*

Society, Jul.-Dec. 2016.

604 Tradução livre do autor: "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".

605 Disponível em: http://unesdoc.unesco.org/images/0025/002539/253952E.pdf. Acesso em: 27 set. 2017.

606 Tradução livre do autor: "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".

607 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.

608 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 em: http://economia.ig.com.br/2017-11-06/deepmind-inteligencia-artificial.html. Acesso em: 25 mai. 2017.

609 Disponível em: https://futureoflife.org/ai-principles. Acesso em: 25 mai. 2017.

610 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 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 AI 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 AI altamente avançados deve respeitar e melhorar, em vez de subverter, os processos sociais e cívicos dos 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 estar sujeitos a planejamento e mitigação de esforços proporcionais ao impacto esperado. 22) Autoaperfeiçoamento recursivo: sistemas de AI concebidos para automelhorar recursivamente ou autorreplicar 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) Bem 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.

611 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".*

612 Disponível em: http://unesdoc.unesco.org/images/0025/002539/253952E.pdf. Acesso em: 25 mai. 2017.

613 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.

614 As características mais utilizadas para o embasamento da personalidade humana são: consciência; racionalidade; autonomia (*self motivated activity*); capacidade de comunicação; e autoconsciência (*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,

2008, p. 141. 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.

615 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. 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 autodeterminar, 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.

616 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.

617 VLADECK, 2014.

618 Tradução livre do autor: "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 autosseguro. 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".

619 CASTRO, 2009.

620 O conceito jurídico de pessoa é mutável e está em constante evolução. Por exemplo, os

afrodescendentes 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, 2009.

621 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 genuíno. Por conta disso, o jus-filósofo italiano Ugo Pagallo denomina isso de "autonomia artificial".

622 CASTRO, 2009.

623 Esse fenômeno jurídico é também denominado por outros autores como *problem of the many hands* ou *accountability gap*.

624 MULHOLLAND, 2009.

625 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.

626 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.

627 Disponível em: http://img.rtp.pt/icm/noticias/docs/6c/6c3203f10cc5377801aae1c0d1b8ce13_467b87e0a1eaa0377cb70477245debc3.pdf. Acesso em: 25 mai. 2017.

628 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.

629 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 devem ser pagas contribuições periódicas 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) criar um status legal específico para robôs para que, ao 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 aplicar personalidade eletrônica aos casos em que os robôs tomam decisões autônomas inteligentes ou, de outra forma, interagem com terceiros independentemente”.

630 SOLUM, Lawrence. Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, v. 70, 1992. Disponível em: http://scholarship.law.unc.edu/nclr/vol70/iss4/4. Acesso em: 25 mai. 2017.

631 Tradução livre do autor: “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".

632 Defende-se aqui que o consenso seja construído nos moldes propostos por Jürgen Habermas através de embates dialógicos na esfera pública.

633 *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.

634 AMARAL, 2015, p. 94.

3.5. Direito como metatecnologia: o desafio do *Rule of Law* em um mundo tecnorregulado

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"[635]. Anos antes, na obra *Code 2.0*, o professor de Harvard e especialista em tecnologia Lawrence Lessig já havia decretado: *"Code is Law"*[636]. 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 a 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, imprimindo 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 xeque 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 as políticas públicas, desempenhando um novo papel na indução de comportamentos e tomadas de decisão[637].

Apesar de este 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 desempenhar nesse contexto, como ferramenta regulatória e indutora de comportamentos, visando à paz social.

Segundo o teórico italiano de Direito e Tecnologia, Ugo Pagallo[638]:

> *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*[639].

Para Pagallo, estamos vivenciando hoje um cenário de mercantilização de dados pessoais que trafegam online e de forte tecnorregulação, sem que haja um balizamento ético-jurídico satisfatório para a proteção dos direitos constitucionais[640].

Apesar de regulações da internet, como o Marco Civil, e da privacidade, como a LGPD no Brasil, tentarem valorizar o potencial da internet e regular práticas que busquem proteger direitos

constitucionais, a autorregulação tecnológica baseada no design do código[641] simplesmente se sobrepõe à 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[642-643].

Segundo Pagallo[644]:

> *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"*[645].

A tecnorregulação 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[646].

Segundo Lawrence Lessig[647]:

> *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*[648]*. 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*[649-650].

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 tecnorregulado regido pela 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*[651] (ou Estado de Direito)[652] 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 ideia 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[653-654].

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 ideias inter-relacionadas, da seguinte forma: primeiro é responsável por limitar o poder do 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[655]. Embora Bingham considere o conceito como algo idealizado, o autor entende que é um ideal que vale a pena 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[656] 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 os 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"[657].

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 tecnorregulação dos cidadãos realizada em plataformas digitais, englobando seus produtos e serviços oferecidos aos usuários[658].

A regulação algorítmica de dispositivos e plataformas restringe o usuário àquilo 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 serem

responsabilizadas perante o usuário. É a tecnorregulação que se sobrepõe ao Estado Democrático de Direito.

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 tecnorregulatório, 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 tecnorregulação 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 tecnorregulação 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[659].

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 metatecnologia[660].

Para evitar um cenário de tecnorregulação (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 metatecnológica do Direito[661].

As maneiras diferentes em que podemos entender os propósitos normativos da lei como uma metatecnologia nos levam a expandir nossa visão jurídica tradicional. Por exemplo, uma abordagem metarregulatória 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 o advento de novos problemas legais, por exemplo, novos *hard cases*[662].

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 tecnorregulação, ampliados pela disseminação do ambiente de IoT, o *Rule of Law* deve ser visto como a premissa para o desenvolvimento tecnológico, ou como uma metatecnologia, 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.

Com relação ao papel do Direito, declara Paul Ohm[663]:

> *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*[664].

Para que o direito atue adequadamente como metatecnologia, deve estar lastreado por diretrizes éticas condizentes com a era da hiperconectivade. Nesse sentido, o avanço tecnológico deve ser guiado através de uma perspectiva centrada no ser-humano, mas que consiga compreender a capacidade de influência dos agentes não humanos, visando a 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[665]:

> *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*[666-667].

O Direito, lastreado por um embasamento ético adequado, servirá como um canalizador do processamento de dados e demais materialidades tecnológicas evitando uma tecnorregulação nociva à humanidade. Nesse novo papel, é importante que o Direito oriente a produção e o 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[668].

Segundo Peter Verbeek[669]:

> *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*[670].

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 caso o limite tolerável seja ultrapassado[671]. 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, TOR, é um software orientado pelo valor da privacidade com *privacy by design*. Uma arma que só dispara com a leitura da biometria do dono ou outra técnica similar (*smart gun*) 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*. Recentemente a empresa Amazon desenvolveu uma ferramenta para seu *bot* Alexa denominada *politeness feature*[672], que possui exatamente essa função de ajudar os pais a educarem seus filhos através da interação comunicativa com a Alexa, embutindo o valor da ética no próprio design do produto.

Apesar de isso ensejar debates legítimos sobre paternalismo jurídico, ético e tecnológico, o recurso do Direito como metatecnologia e regulação *by design* se mostra cada vez mais necessário para evitar uma tecnorregulação nociva e demais violações a direitos humanos a partir das novas tecnologias. Por isso, os parâmetros, para serem política e juridicamente legítimos, devem ser fruto de um intenso debate na esfera pública, de modo a espelhar a vontade e a autonomia da sociedade. A regulação *by design* vai exigir, ainda, uma aproximação mais intensa da sociedade com o trabalho dos engenheiros, devendo isso ser visto como algo importante e benéfico para o bom desenvolvimento da Era da inteligência artificial e IoT.

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 as 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.

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[673].

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 influenciar nossa agência.

Verbeek revela uma nova direção para essa discussão sobre como devemos abordar a tecnologia em termos de moralidade. Uma vez que a autonomia de robôs e outras Coisas é suscetível ao crescimento, a sua regulamentação ética terá de cada vez mais 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 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 o 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 das 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 sejam preservadas a autonomia, a privacidade e a segurança do usuário.

Considerando a importância do Direito como um sistema (ou ferramenta; tecnologia) eficaz para se regularem ações e nortearem 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 metatecnologia, 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[674], 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 a maioria das atividades on-line são de tipo comercial e que a Web é considerada como uma gigantesca mina de dados pessoais, fatores 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[675].

Para otimizar o efeito positivo e minimizar os danos oriundos do efeito disruptivo da regulação tecnológica avançada, é crucial que se compreendam seus impactos e consequências, considerando os aspectos técnicos e peculiaridades das novas formas de comunicação e, também, de regulação.

---

635 FLORIDI, Luciano. *The Fourth Revolution*: how the infosphere is reshaping human reality. Oxford: Oxford University Press, 2016.

636 LESSIG, Lawrence. Code is Law: on liberty in cyberspace. *Harvard Magazine*, 2000. Disponível em: http://harvardmagazine.com/2000/01/code-is-law-html. Acesso em: 24 mai. 2017.

637 Disponível em: https://perma.cc/C64Z-JJMD. Acesso em: 24 mai. 2017.

638 PAGALLO, 2013.

639 Tradução livre do autor: "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".

640 PAGALLO, 2013.

641 A expressão "design de código" aqui se refere à arquitetura da tecnologia, abrangendo não apenas o software através de design algorítmico, mas também a arquitetura de software, como afirma 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"*. LESSIG, 2000.

642 PAGALLO, Ugo *et al*. New technologies and law: global insights on the legal impacts of technology, law as meta-technology and techno regulation. 2015. Disponível em: https://www.lawschoolsgloballeague.com/wp-content/uploads/2017/01/New-Technologies-and-Law-Research-Group-Paper-2015.pdf.

643 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 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.

644 PAGALLO *et al.*, 2015.

645 Tradução livre do autor: "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 tecnorregulatório, 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 tecnorregulação 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'".

646 PAGALLO *et al.*, 2015.

647 LESSIG, Lawrence. *Code*: version 2.0. New York: Basic Books, 2006.

648 Ver: LESSIG, 2000.

649 A crítica à arquitetura algorítmica neste texto também pode ser expandida para

arquitetura de hardware.

650 Tradução livre do autor: "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".

651 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.

652 Usaremos ambos os termos como sinônimos neste trabalho.

653 BINGHAM, Tom. *The Rule of Law*. London: Penguin, 2010.

654 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.

655 BINGHAM, 2010.

656 Disponível em: http://www.unrol.org/files/2004%20report.pdf. Acesso em: 26 set. 2017.

657 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.

658 BINGHAM, 2010.

659 PAGALLO, Ugo. Cracking down on autonomy: three challenges to design in IT Law. *Ethics and Information Technology*, vol. 14, n. 4, 2012.

660 PAGALLO *et al.*, 2015.

661 Disponível em: https://plato.stanford.edu/entries/rule-of-law. Acesso em: 24 mai. 2017.

662 PAGALLO, Ugo; DURANTE, Massimo. The pros and cons of legal automation, and its governance. *European Journal of Risk Regulation*, vol. 7, n. 2, 2016.

663 OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, v. 57, p. 6, 2010.

664 Tradução livre do autor: "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".

665 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.

666 Tradução livre do autor: "Como profissionais centrados no ser humano, temos uma tremenda oportunidade de moldar um mundo mais humanista e inclusivo em conjunto com a AI, 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 AI 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".

667 Disponível em: https://weforum.ent.box.com/v/AI4Good?platform=hootsuite. Acesso em: 24 mai. 2017.

668 FLORIDI, 2016.

669 VERBEEK, 2011.

670 Tradução livre do autor: "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*".

671 Disponível em: http://g1.globo.com/Noticias/Carros/0,,MUL1286685-9658,00.html. Acesso em: 24 mai. 2017.

672 Disponível em: https://www.independent.co.uk/life-style/health-and-families/amazon-alexa-reward-polite-children-manners-voice-commands-ai-america-a8325721.html. Acesso em: 10 nov. 2018.

673 VERBEEK, 2011.

674 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.

675 Discurso no 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.

Conclusão

"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 transmitida ao vivo entre dois *Home Bots*, 2017)

A Era da Internet das Coisas (IoT) e da Inteligência Artificial, composta por um complexo ecossistema de computação ubíqua e intensa interação entre agentes humanos e não humanos (cada vez mais autônomos e menos previsíveis), nos convida a refletir profundamente sobre os rumos da nossa sociedade e sobre quais lentes são mais adequadas para se analisar esse contexto de hiperconectidade.

Esse novo cenário tecnológico, por um lado, pode gerar grandes benefícios ao desenvolvimento econômico e social. Por outro, impõe novos desafios constitucionais e democráticos que não devem ser subestimados ou negligenciados.

Vivemos hoje em um mundo de dados, gerados e tratados de forma intensa por humanos e máquinas sem haver por vezes uma tutela jurídica adequada do cidadão para garantir a segurança e o sigilo de suas informações ou para coibir abusos com relação ao tratamento

dos seus dados pessoais. Conforme exploramos nesta obra, isso pode derivar de diferentes fatores como, por exemplo: falta de regulação adequada; falta de *enforcement* das legislações vigentes; ou por falta de consciência crítica e capacitação dos cidadãos nos temas relacionados às novas tecnologias e à proteção dos dados pessoais.

Para que cheguemos a uma regulação jurídica adequada e democraticamente legítima é importante debatermos as noções de privacidade, proteção de dados e ética que deverão nortear os avanços tecnológicos, refletindo sobre o mundo em que queremos viver e em como nos enxergamos nesse novo mundo de dados e máquinas cada vez mais inteligentes relacionado ao novo cenário de IoT.

A intensificação da interação homem-máquina e de decisões algorítmicas exigem novas lentes ontológicas e epistemológicas capazes de compreender melhor a influência desses elementos na nossa esfera privada e na esfera pública conectada, além da necessidade de uma eficaz governança de dados.

Defendemos nesse trabalho que as Coisas são dotadas de poder de agência e têm interagido com seres humanos de forma cada vez mais autônoma e imprevisível devido a técnicas de *machine learning*, entre outras. Com a tecnologia passando de simples ferramenta a agente influenciador e tomador de decisões, o direito deve reconstruir-se no mundo tecnorregulado, incorporando esses actantes a partir de um viés “meta” (como uma metatecnologia), construindo as bases normativas para uma regulação ética das novas tecnologias através do design.Para tanto, devemos aprimorar e fomentar modelos de design de tecnologia centrados no ser humano (*human-centered design*) e sensíveis a valores constitucionais, regulando, por exemplo, ética, segurança e privacidade por meio do

design (o que denominamos nesta obra de “design sensível a valores” ou, em inglês, *value sensitive design*).

O direito deve estar atento ao seu papel nesse cenário para, de um lado, não obstaculizar demasiadamente o desenvolvimento econômico e tecnológico em andamento e, do outro lado, regular com eficácia as práticas tecnológicas, visando a coibir abusos e protegendo os direitos vigentes. Benefícios e riscos para empresas, Estado e cidadãos devem ser sopesados de forma cautelosa, por meio de uma perspectiva de garantia de direitos fundamentais. A regulação jurídica nesse momento exige uma reflexão ética e democrática que a guie adequadamente. Somente através de uma pavimentação ética adequada conseguiremos garantir um avanço positivo deste novo mundo de dados fortemente impactado pelas características da IoT e da Inteligência Artificial.

Referências

ABBATE, Janet. *Inventing the internet*. Cambridge: 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.

ACCENTURE. *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. Discourse/materiality. *In*: ARADAU, Claudia *et al. Critical security methods: new frameworks for analysis*. New York: Routledge, 2014, p. 57-84.

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 futuro 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. Durham: 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: 7 fev. 2017.

BAPTISTA, Rodrigo. Porque a Internet das Coisas implica em gerenciar contextos, e não dados. *Computerworld*, 2 jul. 2015. Disponível em: https://computerworld.com.br/2015/07/02/porque-internet-das-coisas-implica-em-gerenciar-contextos-e-nao-dados. Acesso em: 31 mar. 2017.

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. *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.

BESSIS, Nik; 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*. London: 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.

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. Acesso em: 2 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.

BRILL, Mark. 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: 2 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*. Cambridge: 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: 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: Egg Minder. *Meio Bit*, nov. 2013. Disponível em: http://meiobit.com/271383/thinkgeek-egg-minder-smart-bandeja-pra-ovo. Acesso em: 31 jan. 2017.

CASTELLS, Manuel. *A Sociedade em Rede — A Era da Informação*: Economia, Sociedade e Cultura. Vol. I. São Paulo: Paz e Terra, 1999.

CASTRO, Marco Aurélio. Personalidade jurídica do robô e sua efetividade no Direito. Tese (Doutorado). Universidade Federal da Bahia, 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.

CAVALIERI FILHO, Sérgio. O direito do consumidor no limiar século XXI. *Revista de Direito do Consumidor*, nº 35, p. 105, jul./set. 2000.

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. The internet before commercialization. In: CERUZZI, Paul; ASPRAY, William (Eds.). *The internet and american business*. Cambridge: The MIT Press, 2008.

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.

CHAUI, Marilena. *Convite à filosofia*. 14. ed. São Paulo: Ática, 2010.

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.

COLE, George S. Tort liability for Artificial Intelligence and expert systems. *Computer/Law Journal*, vol. 10, n. 2, 1990.

CONCEITO.DE. *Conceito de tecnologia*, 15 ago. 2011. 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.

CORREIO DO POVO. 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: 7 ago. 2017.

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; 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: 3 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: 5 jul. 2017.

DHANJANI, Nitesh. *Abusing the Internet of Things*: blackouts, freakouts, and stakeouts. Newton: O'Reilly Media, 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: https://www.dn.pt/sociedade/interior/tay-a-inteligencia-artificial-racista-e-cheia-de-odio-da-microsoft-voltou-a-aparecer-5102581.html. Acesso em: 16 ago. 2017.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

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 A. F. What is algorithm governance? *IEEE Internet Computing*, v. 20, p. 60, 2016.

DORADOR, Marcelo. Inauguração do Centro Integrado de Monitoramento em SBC. *ABC do ACB*, 2 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. *ComputerWorld*, 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 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.

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.

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: Edições 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. 2016a. Disponível em: https://www.onthewire.io/ftc-warns-of-security-and-privacy-risks-in-iot-devices. Acesso em: 31 jan. 2017.

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.

FISCHER-HÜBNER, Simone; WRIGHT, Matthew (Eds.). 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: Oxford University Press, 2016.

FOLLETT, Jonathan. *Designing for emerging technologies*: UX for genomics, robotics, and the Internet of Things. Newton: O'Reilly Media, 2014.

FORTES, Vinicius Borges. *Os direitos de privacidade e a proteção de dados pessoais na internet*. Rio de Janeiro: Lumen Juris, 2016.

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 materialist social inquiry: designs, methods and the research-assemblage. *International Journal of Social Research Methodology*, v. 18, n. 4, p. 399-414, 2015.

FRANKENA, William K. *Ética*. 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.

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*. New 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.

GALIMBERTI, Umberto. *The human being in the age of technique*. São Leopoldo: 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: 8 mai. 2017.

GILCHRIST, Alasdair. Introducing Industry 4.0. *Industry 4.0*. New York: Apress, 2016.

GILLESPIE, Tarleton. The relevance of algorithms. *In*: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo J.; FOOT, Kirsten A. (Eds.). *Media technologies*: essays on communication, materiality, and society. Cambridge: 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: 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.

HABERMAS, Jürgen. *The Theory of Communicative Action*: reason and the rationalization of society. Vol. 2. Cambridge: Polity Press, 1986.

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*: HARAWAY, Donna. *Simians, cyborgs, and women*: the reinvention of nature. New 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 autorregulação pelo código: características, impacto e limites de um novo modelo. In: LEAL, Fernando (Org.). *Direito privado em perspectiva*. São Paulo: Malheiros, 2016, v. 1.

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: 8 fev. 2017.

HOEPMAN, Jaap-Henk. Privacy design strategies. *In*: CUPPENS-BOULAHIA, Nora *et al*. (Eds.). *ICT systems security and privacy protection*. New York: Springer, 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*: VASCONCELOS, Fernando Antônio de; KNOERR, Viviane Coêlho de Séllos; MARTINS, Fernando Rodrigues (Coords.). *Direito do consumidor I* [Recurso eletrônico on-line]. Florianópolis : CONPEDI/UFPB, 2014, p. 147.

HOWARD, Philip. *Pax technica*. 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 responsabilidade*: ensaio de uma ética para a civilização tecnológica. Rio de Janeiro: Contraponto, 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. Lisboa: Edições 70, 2008.

KANT, Immanuel. *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; 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 systems. San Rafael: 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: 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.

LATOUR, Bruno. *Ciência em ação*: como seguir cientistas e engenheiros sociedade afora. Trad. Ivone C. Benedetti. São Paulo: Editora UNESP, 2000.

LATOUR, Bruno. *Jamais fomos modernos*: ensaio de antropologia simétrica. Trad. Carlos Ireneu da Costa. São Paulo: Editora 34, 1994.

LATOUR, Bruno. On technical meditation: philosophy, sociology, genealogy. *Common Knowledge*, v. 3, n. 2, p. 29-64, 1994.

LATOUR, Bruno. *Reassembling the social*: an introduction to actor-network theory. Oxford: Oxford University Press, 2005.

LATOUR, Bruno; WOOLGAR, Steve. *Laboratory life*: the construction of scientific facts. Princeton: Princeton University Press, 1986.

LAW, John; LODGE, Peter. *Science for social scientists*. London: Macmillan, 1984.

LAW, John; SINGLETON, Vicky. Performing technologies' stories: on social construtivism, performance, and performativity. *Technology and Culture*, v. 41, n. 4, p. 765-775, oct. 2000.

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: 4 mai. 2017.

LEMKE, Thomas. New materialisms: Foucault and the 'government of things'. *Theory Culture & Society*, apr. 2014.

LEMOS, André. *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; SOUZA, Carlos Affonso. *Marco Civil da Internet*: construção e aplicação. Juiz de Fora: Editar, 2016.

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: 5 jan. 2017.

LESSIG, Lawrence. *Code*: and other laws of cyberspace. New York: Basic Books, 1999.

LESSIG, Lawrence. Code is law: on liberty in cyberspace. *Harvard Magazine*, 2000. Disponível em: http://harvardmagazine.com/2000/01/code-is-law-html. Acesso em: 24 mai. 2017.

LESSIG, Lawrence. *Code*: version 2.0. New York: Basic Books, 2006.

LI, Shancang; XU, Li. *Securing the Internet of Things*. Cambridge: Syngress, 2017.

LIDDELL, Henry; SCOTT, Robert. *Greek-english lexicon*. 7. ed. Oxford: Oxford University Press, 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, 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; 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: 8 fev. 2017.

MACEDO, Maria Fernanda Gonçalves; BARBOSA, A. L. Figueira. *Patentes, pesquisa & desenvolvimento*: um manual de propriedade industrial. Rio de Janeiro: Fiocruz, 2000.

MACEDO JÚNIOR, Ronaldo Porto. Privacidade, Mercado e Informação. *Justitia*, São Paulo, n. 61, p. 245-259, jan./dez. 1999.

MCEWEN, Adrian; CASSIMALLY, Hakim. *Designing the Internet of Things*. Hoboken: John Wiley & Sons, 2013.

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: 7 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, 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.

MAGRANI, Eduardo. *Democracia conectada*: a internet como ferramenta de engajamento político-democrático. Curitiba: Juruá, 2014.

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, Gary. What's in a name? Some reflections on the sociology of anonymity. *The Information Society*, v. 15, n. 2, p. 99-112, May 1999.

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: 7 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.

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; 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*, Jul.-Dec. 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: 2 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: 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 Sampaio. 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*, v. 15, p. 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.

O'REILLY, Tim. 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*, 9 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. *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: 5 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. Acesso em: 25 jan. 2017.

OTTERLO, Martijn van. A machine learning view on profiling. In: HILDEBRANDT, Mireille; DE VRIES, Katja (Eds.). *Privacy, due process and the computational turn*: philosophers of law meet philosophers of technology. Abingdon: Routledge, 2013.

PAGALLO, Ugo. Cracking down on autonomy: three challenges to design in IT law. *Ethics and Information Technology*, vol. 14, n. 4, 2012.

PAGALLO, Ugo. *The laws of robots*: crimes, contracts, and torts. Dordrecht: Springer, 2013.

PAGALLO, Ugo *et al*. New technologies and law: global insights on the legal impacts of technology, law as meta-technology and techno regulation. 2015. Disponível em: https://www.lawschoolsgloballeague.com/wp-content/uploads/2017/01/New-Technologies-and-Law-Research-Group-Paper-2015.pdf.

PAGALLO, Ugo; DURANTE, Massimo. The pros and cons of legal automation, and its governance. *European Journal of Risk Regulation*, vol. 7, n. 2, 2016.

PARISER, E. *The filter bubble*: what the internet is hiding from you. New York: Penguin, 2011.

PARIKKA, Jussi; TIAINEN, Milla. What is new materialism. Opening words from the event New Materialisms and Digital Culture. Anglia Ruskin University, 21-22 jun. 2010.

PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: 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: PHILPOTT, Jeremy; 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: Wolters Kluver, 2014.

POWLES, Julia; JUDGE, Jenny. Internet das Coisas ou das pessoas? Trad. Rafael A. F. Zanatta. *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: 7 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*. Cambridge: Harvard University Press, 1971.

RAWLS, John. *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 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.

REDAÇÃO OLHAR DIGITAL. 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 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.

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*. 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.

RODOTÀ, Stefano. *Il mondo nella rete*: quali i diritti, quali i vincoli. Roma: Laterza. 2014.

RODOTÀ, Stefano. 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.

RODOTÀ, Stefano. *Iperdemocrazia*. Roma: Laterza, 2013.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de 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.

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.

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/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.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: Civilização Brasileira, 1993.

SANDEL, Michael. *Justiça*: o que é fazer a coisa certa? Rio de Janeiro: Civilização Brasileira, 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.

SANTOS, Boaventura de Souza. *A nova Tese Onze*. 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: 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.

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.

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.

SOLUM, Lawrence. Legal personhood for artificial intelligences. *North Carolina Law Review*, v. 70, 1992. Disponível em: http://scholarship.law.unc.edu/nclr/vol70/iss4/4. Acesso em: 25 mai. 2017.

SOUZA, Carlos Affonso. O progresso tecnológico e a tutela jurídica da privacidade. *Direito, Estado e Sociedade*, n. 16, p. 8, jan./jul. 2000.

SOUZA, Carlos Affonso Pereira de; FRANCISCO, Pedro; MACIEL, Marília. Marco Civil da Internet: uma questão de princípio. Cadernos Colaborativos FGV Direito Rio, 2011.

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.

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.

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*, 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.

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: 2 mai. 2017.

VERBEEK, Peter. *Moralizing technology*: understanding and designing the morality of things. Chicago: 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, 2015.

WALLACE, K.A. Anonymity. *Ethics and Information Technology*, v. 1, n. 1, p. 23-35, 1999.

WALLACE, K.A. On-line anonymity. *In*: TAVANI, Herman; HIMMA, Ken (Eds.). *Handbook on information and computer ethics*. Hoboken: John Wiley & Sons, 2008.

WALLACH, Wendell *et al*. *Artificial intelligence for 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: Oxford University Press, 2008.

WANG, Yongheng; ZHANG, Xiaoming (Eds.). *Internet of Things*: International Workshop, IOT 2012, Changsha, China, August 17-19, 2012. New York: Springer, 2012.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890.

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*: TURNER, Bryan S. (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.

WIGGERSHAUS, Rolf *et al*. *The Frankfurt School*: its history, theories, and political significance. Cambridge: The MIT Press, 1995.

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. New York: 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.

ZANATTA, Rafael A. F. *O utilitarismo de Jeremy Bentham*. 2010. Disponível em: https://rafazanatta.blogspot.com.br/2010/04/o-utilitarismo-de-jeremy-bentham.html. Acesso em: 20 set. 2017.

ZIEGELDORF, Jan; MORCHON, Oscar; WEHRLE, Klaus. Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, v. 7, n. 12, p. 2728-2742, 2013.

Posfácio

Entre leões africanos (em tempos de *deep fake*, os registros fotográficos estão disponíveis para *fact-checking* caso alguém duvide), estive com Eduardo Magrani pela primeira vez em 2016. Evidentemente já conhecia e acompanhava o seu trabalho, mas este primeiro contato pessoal se deu quando a *Law Schools Global League,* através de seu Grupo de Trabalho em Novas Tecnologias e Direito, promoveu o seu 2º Workshop sobre Novas Tecnologias e Direito, em uma parceria com a Universidade de Pretória, reunindo ali no forte verão sul-africano pesquisadores da área vindos de diversas partes do mundo.

Coordenado pelos queridos professores Ugo Pagallo e Mónica Guise Rosina, expoentes desta área por quem fomos selecionados para participar da iniciativa, o exercício foi sensacional. Cada participante levou uma proposta de texto razoavelmente desenvolvida sobre o tema de seu interesse, e ao longo dos encontros discutíamos, debatíamos, criticávamos e apontávamos fragilidades e caminhos de melhoria uns nos textos dos demais, de modo que, ao final da semana de colaboração, cada um tinha contribuições para um texto muito mais maduro, muito mais sólido, resistente e bem mais encorpado.

Em seu soneto mais célebre, meu conterrâneo Augusto dos Anjos, o maior poeta parnasiano do Brasil, eleito o Paraibano do Século 20, vaticina que “O Homem, que, nesta terra miserável, mora entre feras, sente inevitável necessidade de também ser fera”.

Contrariando a normalmente aguçadíssima percepção humana do genial autor de *Eu e outras poesias,* nem leões africanos, nem a obsessão angustiada dos companheiros da semana em chegar ao formato perfeito para o trabalho em um par de dias, nada abalava a leveza de espírito de Eduardo Magrani. Em uma semana de convivência, descobri um colega disposto ao debate sempre no mais alto grau de lealdade intelectual, de espírito colaborativo como a essência do mundo, dos *commons* e da própria internet em que ele acredita, que não se pronunciava se não tivesse algo verdadeiramente intrigante a dizer ou a somar, que se recusava a tecer uma crítica se não encontrasse uma forma gentil, construtiva e respeitosa de fazê-lo, e que sobretudo esbanjava a elegância da simplicidade reservada às almas verdadeiramente iluminadas.

Reza a lenda em Western Cape que, antes de retornar ao Rio de Janeiro, Eduardo Magrani ainda partiu de Pretória para enfrentar as águas de *Gangsbaai* e nadar entre os grandes tubarões brancos, cedendo afinal à inevitável necessidade parnasiana de também ser fera. Ainda avaliei os riscos da empreitada, mas preferi visitar uma vinícola. Soou mais adequado ao meu perfil. Não nos encontramos mais pessoalmente por um bom tempo, mas, apesar disso, neste novo mundo hiperconectado, a distância já não foi capaz de nos impedir de trabalhar juntos em um bom número de projetos e iniciativas interessantes. De toda maneira, havia nascido ali uma admiração que me envaidece quando suponho que seja mútua e que para mim não significava apenas acompanhar o seu trabalho e me inquietar com as suas reflexões, mas também o privilégio de chamá-lo de amigo.

No texto que conheci na África do Sul, Eduardo Magrani já havia plantado e regado com cuidado as sementes de vários dos elementos

que posteriormente viriam a germinar e a ser minuciosamente analisados na árvore frondosa em que se converteu *Entre dados e robôs: ética e privacidade na era da hiperconectividade*. Finalizada, é hora de a obra dar sombra e frutos ao debate técnico-científico, regulatório-estratégico e sociocultural para a área no Brasil.

Dificilmente alguém que não conviva com a ansiedade de produzir e publicar textos em uma área com a dinâmica deste diálogo entre direito, tecnologia e sociedade alcançará compreender o grau de dificuldade que a tarefa encerra. Instável, absolutamente imprevisível e apaixonante — exatamente como o meu Treze Futebol Clube —, o tema é vulcânico.

O pesquisador que acompanha de forma minimamente atenta os desdobramentos de saberes de ritmo semelhante haverá de se deparar todos os dias com dezenas, quando não centenas de novos textos sobre a temática, análises, comentários, eventos, reportagens, relatórios, informes, descobertas, projetos, normas, entrevistas, iniciativas públicas, privadas e multissetoriais diversas, o que torna quase impossível o trabalho de acompanhar, curar, avaliar e refletir sobre este volume de informação nova, ainda que seja tão somente para identificar o que realmente merece destaque e é relevante. E, se estamos falando em produzir uma tese doutoral sobre este tema, some-se a isso a exigência de uma habilidade extra para delimitar um objeto de investigação que tenha não apenas o aspecto de originalidade que dele se espera, mas principalmente fôlego e densidade para se manter original durante o tempo que a pesquisa consumir — e preferencialmente um pouco mais além.

É desumano.

É uma tarefa que exige, além de talento e competência, compromisso absoluto e disciplina espartana.

Há duas receitas relativamente fáceis para conquistar popularidade imediata no tema que Eduardo Magrani finalmente escolheu para seu trabalho e para esta obra. Uma é o discurso inocente e pouco responsável de que os avanços da conectividade são exclusivamente benéficos, que desenvolvimento tecnológico traz consequências quase que unicamente positivas, e de que os efeitos colaterais ou não existem ou são desprezíveis. A simpatia da evangelização pelo solucionismo tecnológico é imediata. A outra é o tom alarmista, apocalíptico, quase conspiratório, de que é preciso resistir a qualquer custo a avanços que praticamente não trazem perspectivas de aprimoramento econômico, social ou humano, de que tudo o que os governos querem é o controle das mentes, tudo o que a indústria deseja é o controle dos cofres, e de que o indivíduo só tem a perder neste mundo em rede que se desenha diante de nossos olhos. O discurso do medo também tem seus adeptos de primeira hora. E estas são receitas fáceis, não nos enganemos, porque são caminhos errados, que por falta de visão não compreendem ou que por malícia negligenciam a sofisticação das diversas questões que se entrelaçam e que precisam ser consideradas quando alguém se debruça sobre este tema.

Uma alternativa, muito mais trabalhosa, que envolve muito mais esforço, disponibilidade e honestidade intelectual para enfrentar a complexidade de que se reveste o tema, é considerar todas as variáveis que o trabalho puder alcançar, cotejá-las individualmente e em diferentes contextos, procurar estabelecer pontos de equilíbrio, convergência, ou mesmo *red lines* para situações extremas, usar ferramentas diversas para avaliar os cenários críticos, recorrer à análise jurídica, regulatória, mas também explorar a abordagem

ética da questão, enfim, dar-se ao trabalho de não simplificá-la de maneira inconsequente e inadequada.

E eu não esperaria outro o caminho a ser escolhido por Eduardo Magrani.

É o caminho escolhido quando o autor se preocupa em revisitar o conceito de privacidade à luz das novas características da rede de dispositivos que se convencionou denominar de Internet das Coisas (IoT). Na verdade, as coisas da Internet das Coisas não são coisas: são sensores — por mais sexy que a expressão, pela razão e pela forma como foi cunhada, possa aparentar. E porque elas são sensores cada vez mais comuns, pervasivos, próximos e incorporados ao cotidiano do indivíduo, representam risco potencial muito maior para a proteção de seus dados pessoais, da sua privacidade, do seu direito de autodeterminação informativa. Lidar com estes dispositivos exige um cuidado muito maior do que lidar com coisas, nessa perspectiva semântica mais pura. É preciso considerar a IoT em função de elementos como infraestrutura, interconectividade e segurança, o que o trabalho faz com critério, ilustrando com exemplos de esforços regulatórios concretos.

É o caminho escolhido com solidez e criatividade teórica, quando o autor recorre à obra de Bruno Latour para mapear e compreender como a associação *indivíduo + artefato técnico* interfere no cotidiano das relações sociais para além da condição individual ou humana, enquanto binômio ao qual se reconhece capacidade de agência conjunta, própria e autônoma.

É, por fim, o caminho escolhido quando Eduardo Magrani explora as várias opções de governança de algoritmos, por ferramentas que vão da técnica à regulação propriamente dita, passando pela ética, padrões de mercado e por alternativas autorregulatórias e

governamentais, sugerindo que estas alternativas podem concentrar esforços em elementos distintos como transparência, responsabilidade ou garantias técnicas, e ainda que sejam calibradas de acordo com fatores como a natureza do algoritmo, o contexto de aplicação, seus riscos e seus usos. De se dar destaque à ressalva da importância não apenas de encontrar responsabilidades pelo manejo destas rotinas computacionais, mas o horizonte mais amplo de se alcançar justiça, para o que entende que é possível caminharmos em direção a um sistema de responsabilidade compartilhada, em um ambiente que, mesmo tecnorregulado, deverá ser centrado na pessoa humana, ao tempo em que seja também sensível a valores.

É necessário o registro de um último esforço de Eduardo Magrani, que nem de longe é menos importante, que é o de linguagem. Quem acompanha intervenções e registros de suas aulas, participações orais e exposições nos diversos espaços que ele ocupa — e ele não só está em toda parte como em todas as plataformas — percebe muito facilmente a sua preocupação em escolher sempre termos simples, linguagem clara, em conversar sem sofisticar o tema quando isso seja desnecessário, em utilizar analogia de cenários familiares e exemplos de casos do cotidiano que possam desmistificar as questões de interesse para o público com quem está interagindo. É uma preocupação nobre e legítima. Este é um tema que já de há muito não deve e não pode ficar restrito à academia, à comunidade técnica ou a intelectuais. Esta esfera pública colonizada por algoritmos com insaciável fome de dados está interconectada via sua dimensão pública, via sua dimensão privada e ainda na intersecção entre as duas. Os efeitos dessa colonização são sentidos no mercado financeiro, no tratamento de saúde, na relação de consumo, na publicidade, na difusão de informações e conteúdo, no uso de

serviços públicos, na educação, na segurança pública, no policiamento de rua, no transporte coletivo, na participação eleitoral, no exercício do debate democrático, enfim, em todos os aspectos da vida de um cidadão comum. É um debate que precisa ser travado em uma linguagem a que esse cidadão tenha alcance, para que ele possa entender, se conscientizar e eventualmente, desejando, aportar as contribuições a que tem direito.

Em uma intervenção oral, Eduardo tem mostrado, esta modulação está mais facilmente ao alcance. O olho no olho, o tom, a intensidade, o gestual, todos os recursos do discurso oral facilitam a simplificação da linguagem para quem tem a intenção de fazê-lo. Mas, na linguagem escrita, num trabalho extenso e de profundidade muito maior, o desafio é enorme. É improvável que alguém desempenhe a tarefa de revisitar o embate filosófico entre o utilitarismo e a deontologia, fundamental para discutir decisões tomadas através de mecanismos e técnicas de inteligência artificial, ou de abordar a automação de aspectos de coercitividade de medidas regulatórias, ou ainda a de descrever desafios técnicos de interoperabilidade para sensores sem escrever com alguma densidade, fora do vocabulário técnico e mais fechado destes domínios do conhecimento.

É improvável, mas é possível.

E o fato de o resultado desta obra ser um exemplo tão positivo de que isto é possível revela também que Eduardo Magrani é um representante credenciado de uma nova academia, não só multidisciplinar, mas multissetorial, que mais do que conversar com outros saberes, compreende que conversar com outros segmentos da sociedade, ter uma mensagem clara para disseminar o conhecimento e fazer essa mensagem atingir uma audiência ampla é chave para

este novo papel do pesquisador menos isolado, mais integrado ao mundo, e que procura combinar as respostas à sua curiosidade com a resposta para grandes problemas coletivos. Em um país como o Brasil, é a sociedade que patrocina grande parte da pesquisa científica, e ela começa a exigir resultados mais objetivos, visibilidade, difusão de informação e sobretudo impacto. A era do hermetismo acadêmico, seja o de linguagem, seja o institucional, acabou. Seu fôlego esgotou-se. Ver surgir esta nova postura mais aberta, mais inclusiva e mais preocupada com impacto efetivo para o cidadão, seguindo com Augusto dos Anjos — que o mote é bom — é presenciar o formidável enterro de sua última quimera — música para os ouvidos de um acadêmico que vive o multissetorialismo.

Uma alegria receber *Entre dados e robôs: ética e privacidade na era da hiperconectividade* como esse sinal de uma energia acadêmica nova, que ao mesmo tempo mantém rigor de abordagem e método, se harmoniza com interesses públicos coletivos e se posiciona de maneira a contribuir com o grande esforço intelectual coletivo de resolver problemas estratégicos nacionais e globais.

Que esta obra e a continuidade do trabalho do autor nos sirvam para construir e para pavimentar a estrada da transição de nossa era para um período no qual o uso massivo e crescente de automação não esteja simplesmente a serviço da vigilância, do controle, acentuando divisões, desequilíbrio e concentração de poder. Que conhecer cada vez mais e melhor as nuances deste movimento seja o instrumento para tomar consciência, construir capacidades, monitorar, agir e exigir avanços técnicos que nos conduzam a desdobramentos positivos, reforcem a cidadania, as liberdades, o combate à corrupção, à exclusão e às desigualdades, numa equação

em que o resultado final seja o desenvolvimento humano justo, sustentável e universal.

Cláudio Lucena

Professor da Faculdade de Direito da Universidade Estadual da Paraíba, pesquisador da Fundação para a Ciência e a Tecnologia de Portugal, afiliado ao Research Centre for the Future of Law da Universidade Católica Portuguesa

ANEXO

Você está sendo (continuamente) observado

No livro *1984*, escrito em 1948 pelo autor inglês George Orwell, a sociedade é controlada por um olhar onipresente e onisciente, que vigia todos em cada momento de suas vidas. Chamado de *The Big Brother* — usando a analogia de um irmão mais velho, que vigia os mais novos —, representaria o próprio Estado totalitário e manipulador. É uma sociedade observada — a frase original que marca a narrativa é: *"The Big Brother is watching you"*, em que cada membro é parte de um todo social, uma massa que se comporta da mesma forma, a fim de dar força ao Estado. O indivíduo deixa de existir como ser único e passa a ser um mero componente do Estado.

Nesse mundo de ficção, a intimidade e a privacidade não são direitos do indivíduo, já que o Big Brother tem seu olhar sobre todos. Não há o direito singular, não existe o segredo, nem a esfera privada, pois todos os passos são monitorados.

Hoje, com a transformação digital trazida e consolidada pela sociedade da informação e da tecnologia, vivemos igualmente uma realidade em que todos observam todos, todo o tempo; celulares, GPS, redes sociais, máquinas de busca, sites de comércio eletrônico e afins tornam a nossa vida mais rápida, mais cheia de informações e de serviços, mas também guardam nossos movimentos e pegadas

virtuais, e não mais nos lembramos como era a vida sem essa transformação digital que tudo vê.

Estamos presentes no mundo virtual tanto quanto estamos no real — é como se houvesse uma realidade paralela, na qual existe um outro (ou vários outros) de cada um de nós. À medida em que somos traduzidos em bits e bytes, tornamo-nos cada vez mais públicos. É pela internet que tomamos conhecimento de notícias, é lá que nos relacionamos com amigos, que encontramos emprego, que planejamos nossas viagens... Enfim, não estar conectado implica ser um *outsider*, um não convencional, à margem, que não se encaixa nos conceitos de normalidade social, a exemplo do conceito trazido por Howard Becker. O preço por esta ousadia, de nos tornarmos parte desse todo, é a perda de uma parte só nossa. Analogamente à sociedade pintada por Orwell, deixamos de ter nossa intimidade e privacidade resguardadas — não mais pelo aspecto coercitivo de um Estado autoritário e explicitamente controlador — mas pela ação, às vezes até imperceptível, de uma sociedade transformada digitalmente. Passamos a legitimar um novo Leviatã, assinando uma nova versão do Contrato Social de Thomas Hobbes: abrimos mão da privacidade de nossos dados pessoais em troca de habitarmos na sociedade digital.

Mesmo quando o indivíduo não revela voluntariamente sua intimidade e privacidade no mundo virtual, arrisca-se a tê-las invadidas. A conectividade que lhe encurta as distâncias e o aproxima do futuro também o deixa a um passo dos olhares inescrupulosos. Valores essenciais ao ser humano, como o direito à vida íntima, tornam-se mais frágeis, vítimas de constantes ameaças e invasões.

Uma das principais consequências disto é que cada um de nós se transforma em produto no novo mercado digital. Nossos dados pessoais, nossa privacidade, passam a ter cada dia mais valor e, consequentemente, são mais e mais cobiçadas. Quem somos, onde vivemos e por onde andamos, do que gostamos e com quem nos relacionamos — tudo isto são informações cruciais digeridas pelos novos modelos de negócios vigentes.

Nesta nova realidade, a fim de que haja equilíbrio entre o indivíduo e o todo, a fim de que se preserve a autonomia que cada um de nós deseja exercer sobre nossos dados pessoais, é imperativo que estes sejam protegidos, durante sua coleta, seu armazenamento e sua manipulação. Considerando que o mundo virtual é também global, essa é uma preocupação não só do Brasil — e diversos países ou grupos econômicos têm iniciado trabalhos de regulação sobre o tema.

Na União Europeia, entrou em vigor, em maio de 2018, o RGPD — Regulamento Geral sobre a Proteção de Dados (ou GDPR, sigla em inglês) — definindo o conceito de dados pessoais, assim como informando claramente sobre sua coleta e estabelecendo, entre outras coisas, que esses dados devem ser usados unicamente para a finalidade originalmente autorizada.

O Brasil, seguindo viés análogo ao europeu, teve sancionada, em agosto de 2018, a LGPD — Lei Geral de Proteção de Dados Pessoais — que deverá entrar em vigor a partir de janeiro de 2020. Até lá, a sociedade terá de se adequar a essa nova lei, ajustando a forma como os dados pessoais serão manipulados, como a intimidade de cada indivíduo será tratada, tendo em mente toda a diversidade de usos existentes quando consideramos o contexto da transformação digital.

Algumas empresas globais já vêm sentindo as mudanças trazidas pela nova legislação: recentemente, o Facebook precisou se defender perante as cortes americanas por não ter protegido a privacidade de seus usuários de modo eficaz.

Cada instituição — pública ou privada, grande ou pequena, com ou sem fins lucrativos — precisará se ajustar a um novo modelo de negócios, em que o uso de informações pessoais deverá seguir padrões rígidos quanto ao seu tratamento, com a estrita anuência de seus titulares. Isto significa custo, recursos, investimento — mas também consolida o respeito e a proteção de bens jurídicos e pessoais.

Estamos só no início. Isto é um processo contínuo, em que se busca o equilíbrio entre direitos protegidos. Vamos continuar sendo surpreendidos por inovações que nos farão repensar a forma como enxergamos os indivíduos, os negócios e a sociedade. Mais do que nunca, os valores éticos e a empatia devem ser adotados também na esfera virtual, como nortes para a construção de relações sustentáveis e mutuamente benéficas.

Claudia Cunha
Professora da CESAR School