Centro Universitário de Brasília – UniCEUB
Faculdade de Ciências Jurídicas e Sociais – FAJS

MARIANA DA COSTA MESQUITA CORRÊA

ALGORITMOS E REGULAÇÃO

Brasília/ DF

2018

MARIANA DA COSTA MESQUITA CORRÊA

ALGORITMOS E REGULAÇÃO

Trabalho de conclusão de curso apresentado ao curso de Direito do Centro Universitário de Brasília – UniCEUB, como um dos requisitos para obtenção de grau de Bacharel em Direito.

Orientador: Luiz Patury Accioly Neto

Brasília/ DF

2018

MARIANA DA COSTA MESQUITA CORRÊA

ALGORITMOS E REGULAÇÃO

Trabalho de conclusão de curso apresentado ao curso de Direito do Centro Universitário de Brasília – UniCEUB, como um dos requisitos para obtenção de grau de Bacharel em Direito

Brasília, _____ de 2018.

_____

Luiz Patury Accioly Neto

_____

Examinador

Brasília/ DF

2018

AGRADECIMENTOS

Gostaria de agradecer, primeiramente, ao meu marido, Fernando, que sempre me incentiva, me dá forças e me lembra de que tudo dará certo. Este trabalho é para você, meu amor.

Agradeço à minha mãe e ao meu pai, que me deram a vida, por terem me apoiado nesta segunda graduação, assim como sempre me apoiaram e me amaram incondicionalmente.

Meus mais sinceros agradecimentos a todos os meus professores, com os quais tive o privilégio de aprender nestes cinco anos de Direito. Voltar à Academia foi muito gratificante e enriquecedor. Neste condão, agradeço em especial ao meu orientador, Professor Patury, que conseguiu fazer com que eu realmente entregasse o melhor de mim.

A Ele, agradeço pelas bênçãos sempre tão generosas.

Por fim, mas não menos importante, sou grata por fazer parte desta espécie tão fantástica e enigmática: a humana, dotada da inteligência que nos faz vencer ao mesmo tempo em que nos faz sucumbir.

RESUMO

O objeto do presente estudo é a força regulatória dos algoritmos, aqui entendidos como o código fonte das novas tecnologias da informação e da comunicação. O objetivo é compreender, primeiramente, se estas possuem, de fato, força normativa. Posteriormente, em havendo, se esta força é democrática ou não. Ainda constitui objetivo deste trabalho estabelecer um panorama geral da regulação sobre o tema no Brasil e demonstrar formas de tornar os algoritmos mais transparente e democráticos. A pesquisa bibliográfica foi o meu escolhido para enfrentar tais questões.

Palavras Chave: algoritmos, regulação, democracia, governança.

SUMÁRIO

INTRODUÇÃO

Certo dia, quase dez anos atrás, eu estava trabalhando quando li uma reportagem sobre os dados que o Google coletava de seus usuários. Seguindo as instruções do jornal, fui me embrenhando por um emaranhado de *links* que me redirecionavam para outras páginas até que consegui acessar tais dados. O Google mantinha uma pasta com todos os meus contatos telefônicos, endereços de e-mail (inclusive dos hospedados por outros servidores), um histórico dos lugares que eu mais frequentava e uma listagem de todos os e-mails que eu já havia trocado desde que começara a usar o Gmail.

Eu já desconfiava da coleta de dados, afinal, uma parte do meu trabalho envolvia escolher as melhores palavras-chave para que o anúncio da empresa onde eu trabalhava aparecesse sempre em primeiro lugar nas buscas do Google. Eu entendia os conceitos de robôs de buscas e algoritmos. Mas, naquela época, eu não tinha ideia da quantidade de informações que a gigante de buscas guardava sobre mim.

Com o passar dos anos, o assunto foi se tornando cada vez mais frequente no dia-a-dia de cada um e a privacidade de dados começou a me inquietar ainda mais. Nasci quando ainda não existia internet, diferente da maioria dos meus colegas de curso. Lembro-me muito bem quando usei a rede mundial pela primeira vez, na casa de um tio. A exposição em redes sociais, para mim, não é natural, não é um fenômeno dado.

Iniciei meu trabalho de conclusão de curso tratando sobre o tema da privacidade, mas quanto mais eu pesquisava sobre o assunto, mais me deparava com inúmeras outras tecnologias que, junto com a internet, formam as tecnologias da informação e comunicação (TICs). Em um congresso no Rio de Janeiro, fui apresentada a diversas novas ferramentas recém-criadas pelas gigantes do setor de tecnologia. A cada nova apresentação, eu me dava conta de algo ainda mais profundo e anterior que a questão da privacidade em si. Comecei a perceber a força que os algoritmos têm para regular as vidas humanas.

Escrever sobre tecnologias da informação e comunicação é extremamente desafiador. Ao longo dos quase dois anos escrevendo este trabalho, me deparei com muitas mudanças significativas. No final de 2017, foi anunciado que o *AlphaGo*

Zero tinha estabelecido novos horizontes na área de inteligência artificial, trazendo novos argumentos e questionamentos ao trabalho. Em março de 2018, já com o projeto praticamente finalizado, a Câmara dos Deputados aprovou o Projeto de Lei que regulamenta os aplicativos de mobilidade urbana, como Uber e 99, trazendo uma nova realidade à regulação das TICs no Brasil.

As TICs têm cada vez mais espaço na vida humana. Da residência ao trabalho, passando pelas compras, pelos momentos de lazer e até mesmo durante o sono, aplicativos e objetos inteligentes integram o cotidiano. Diversos avanços têm sido feitos graças à junção das TICs, que vão desde a internet até a inteligência artificial, passando pelo *machine learning,* redes neurais, *Big Data,* entre outros.

As mudanças que circundam o assunto são constantes e, dada a novidade do tema, são também sempre significativas. A cada dia há uma nova descoberta relacionada ao tema. Novas questões são colocadas ao Direito e aos Estados Democráticas na mesma velocidade. Verdadeiras revoluções, que antes levavam décadas, séculos para acontecerem, se dão no espaço de gerações ou até mesmo de anos.

As novas tecnologias, por óbvio, não trazem apenas benesses, exatamente como tudo que é produto do homem. Diversos novos dilemas e paradigmas têm sido criados e o Direito precisa se atentar a isto. A ideia base de todo este trabalho é aquela surgida no congresso no Rio de Janeiro: toda tecnologia traz em si um aspecto regulatório, mas que isto é muito mais forte quando se trata das TICs. Não apenas a arquitetura delas as torna mais aptas a regular, quanto sua presença quase onipresente também potencializa este efeito.

A questão chave discutida neste trabalho é se a substituição, cada vez mais intensa, da lei enquanto força regulatória da humanidade pelo algoritmo que desenha todas essas tecnologias é ou não democrática, dado que a vasta maioria delas são desenhadas pela iniciativa privada.

Questiona-se, ainda, se o formato estatal brasileiro consegue conferir legitimidade às decisões tomadas em todos os poderes, em relação ao assunto principal. A forma como o Brasil tem regulado a matéria é também objeto deste estudo, que tem como método a pesquisa bibliográfica.

Ao tratar de definições técnicas próprias da engenharia computacional, recorri a trabalhos publicados pelas próprias empresas criadoras das tecnologias. Para demonstrar a magnitude, o alcance das TICs nas vidas de cada um, foram utilizados estudos acadêmicos feitos por entes públicos e privados, estudos de casos empresariais, exemplos de fatos concretos que ocorreram durante a pesquisa para este trabalho. Sobre a força normativa dos códigos foram utilizados diversos trabalhos, mas em especial os dos professores doutores Lawrence Lessig, de Harvard e Wolfgang Schulz, da Universidade de Hamburgo.

As referências sobre democracia foram retiradas, principalmente, da obra *Democracy and the limits of self-government* do sociólogo e cientista político Adam Pzreworski. O intuito ao combinar o Direito com a Ciência Política e a Sociologia foi oferecer ao leitor uma pesquisa ampla sobre a relação entre as novas tecnologias, seu aspecto regulatório e democracia, sem se prender em um assunto particular. No entanto, como forma de exemplificação de como a regulação vem sendo feita no Brasil, optou-se por centralizar a análise nas leis e decisões judiciais sobre privacidade de dados, uma vez que inteligência artificial e outros assuntos ainda não são amplamente discutidos pelo Estado brasileiro no âmbito do Parlamento.

Após vasta pesquisa bibliográfica, foi possível concluir que é apenas por meio dos processos democráticos que as TICs conseguirão desenvolver todo seu potencial benéfico. Sem freios e contrapesos, as chances de assistirmos a verdadeiros desastres sociais são grandes. Não é possível, no entanto, precisar para qual lado a balança penderá, ou seja, não é possível saber se as TICs trarão mesmo a revolução que prometem. Quem viver, verá.

1 A PRESENÇA DAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO (TICs) NA SOCIEDADE E SUA IMPORTÂNCIA

Cerca de quinhentos anos antes de Cristo, os chineses criaram um jogo de tabuleiro, extremamente popular na atualidade, chamado Go. O jogo desenvolve o raciocínio lógico e requer análises estratégicas profundas, tendo sido utilizado, segundo relatos históricos, por generais chineses e imperadores para estabelecer estratégias de guerra. O Go é conhecido por sua dificuldade extrema e é até mesmo considerado o jogo mais difícil do mundo (ASSOCIAÇÃO BRASILEIRA DE GO, 2017).

Em maio de 2015, um computador criado pela Alphabet, holding controladora do Google, conseguiu derrotar o melhor jogador do mundo de Go por cem vezes seguidas. Engenheiros da empresa acreditavam que levaria mais dez anos até que isto fosse possível. Para alcançar o feito, os especialistas criaram um *software*, o AlphaGo, que foi alimentado com dados sobre o jogo, como as regras e jogadas possíveis e, utilizando-se deste banco de dados, o *software* aprendeu a jogar (SAMPLE, 2017).

Posteriormente, foi criada uma nova versão do programa, o AlphaGo Zero, que utiliza inteligência artificial (AI). Em outubro de 2017, o *software* conseguiu aprender o jogo sozinho e partindo do zero, sem nenhuma intervenção do homem – não foi necessário que nenhuma pessoa “ensinasse” ao *software* nenhum movimento – e em apenas três dias, o programa não apenas aprendeu todo conhecimento humano a respeito do jogo como desenvolveu jogadas novas e melhores. Enquanto *software*s comuns, como o AlphaGo, precisam de *input* de dados específicos para só então realizar cálculos, os *software*s de inteligência artificial como o AlphaGo Zero realizam sozinhos a busca pelos dados que acharem mais conveniente (SAMPLE, 2017).

O meio científico já se adiantou para classificar o evento como um enorme avanço no campo da inteligência artificial, com vasto potencial em virtualmente todas as áreas do conhecimento. Um dos projetos em andamento na *DeepMind*, braço especializado em inteligência artificial da *Alphabet*, é usar a AI para responder uma pergunta que intriga os cientistas há décadas: o que determina o formato das

proteínas. Os impactos de tal descoberta podem ser tão profundos quanto a cura do câncer (SAMPLE, 2017).

Na Faculdade de Medicina de Columbia, em Nova Iorque, já se utiliza a inteligência artificial para diagnosticar acidentes vasculares cerebrais *antes* que eles ocorram. Na Universidade de Stanford, no Vale do Silício, um sistema de AI obtém diagnósticos dermatológicos acertados em 72% dos casos, contra 66% de precisão dos médicos humanos. A grande diferença entre o sistema criado por Stanford e o da Alphabet é que o primeiro dispõe apenas das informações inseridas nele pelos humanos enquanto que o segundo busca as informações sozinho e consegue identificar o que é, ou não, relevante (MUKHERJEE, 2017).

Todos esses exemplos são viabilizados pela análise feita por inteligência artificial de uma quantidade quase infinita de dados armazenados (DEANGELIS, 2017). E se, atualmente, a humanidade já gera uma quantidade impressionante de informação, no futuro a tendência é que ela seja ainda maior. Em 2015, aproximadamente 7.910 exabites de dados foram produzidos no mundo. Um exabite equivale a um quintilhão de bites. Em termos mais concretos, se um exabite fosse gravado em DVDs e estes fossem armazenados em um avião Boeing 747, seriam necessárias 13.513 aeronaves para se guardar todos os discos. Então, para armazenar DVDs contendo 7.910 exabites de dados, seriam necessários aproximadamente 106 milhões de Boeings 747 (KUNER, CATE, *et al.*, 2012).

Um estudo realizado pela empresa sueca Ericsson mostra que 3,9 bilhões de pessoas estão conectadas à internet por meio de algum dispositivo móvel, que geram dados incessantemente. Em 2022, este número subirá para 6,1 bilhões. Em 2018, espera-se que o número de celulares conectados à internet seja ultrapassado pelo número de outros objetos com a conexão, a chamada Internet das Coisas (*Internet of Things – IoT).* Em 2022, serão 29 bilhões de objetos conectados à rede, sendo 18 bilhões relacionados à IoT (ERICSSON, 2016).

Em outubro de 2017, foi publicado um estudo sobre IoT no Brasil liderado pelo Banco Nacional de Desenvolvimento (BNDES) em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) e realizado pelo consórcio McKinsey, Fundação CPqD e Pereira Neto Macedo Advogados. Nele, estima-se que a IoT tenha um impacto de até 11% do PIB mundial em 2025. Isso representaria um

impacto econômico anual no Brasil de até 200 bilhões de dólares em 2025 (BNDES, MCTIC, 2017).

A Internet das Coisas diz respeito a objetos, que não o celular, conectados à internet e/ou conectados entre si. As implicações são infinitas e alguns resultados já se mostram muito promissores. Na agricultura, sensores espalhados pela lavoura permitem a coleta de informações sobre cada planta, otimizando enormemente o uso de recursos. Temperatura, umidade, pH, luminosidade, nível de irrigação e outros tantos dados são coletados muda a muda possibilitando a redução em 98% da quantidade de agrotóxicos utilizados (MICROSOFT, 2017). Um sensor criado por cientistas brasileiros permite diminuir em 70% o uso de água na lavoura com ganho de 40% de produtividade (AGROSMART, 2017) (SOCIEDADE NACIONAL DA AGRICULTURA, 2014).

Em Lagos, na África, o sistema de IoT da Microsoft permite o gerenciamento da rede de energia de comunidades isoladas, por meio de controle remoto. Painéis captam energia solar, que carregam baterias portáteis. Sensores conectados à internet formam uma rede remota com todas as baterias, permitindo a otimização do sistema, sendo possível prover energia a essas comunidades, que antes eram desprovidas de qualquer fonte energética. Hospitais e escolas estão sendo abastecidos desta forma, evitando o uso de energia gerada por combustíveis fósseis e melhorando a qualidade de vida da população local, que agora tem, por exemplo, acesso a água potável pelo uso de bombas elétricas (MICROSOFT, 2017).

Veículos conectados à internet permitem a coleta de informações em tempo real sobre trânsito, também sendo possível conectar toda a rede de transporte público. Desta forma, é possível fazer desvios de trânsito que diminuam engarrafamentos, assim como disponibilizar mais vagões de metrô para regiões com mais necessidade de forma muito mais rápida (CISCO, 2017).

Na saúde, o monitoramento das condições físicas em tempo real pode diminuir consultas médicas desnecessárias, assim como alcançar diagnósticos mais precisos não apenas do indivíduo, como também de populações inteiras. Os estudos que hoje são feitos com dez mil pacientes, podem ser conduzidos com dados muito mais precisos de milhares de pessoas ao mesmo tempo (IBM, 2017).

Isso tudo só é possível graças ao surgimento e utilização simultânea de várias tecnologias diferentes e complementares. Inteligência artificial, *machine learning,* redes neurais e outras tecnologias, se juntam à internet e, principalmente, ao *Big Data* para promover as intensas mudanças que a humanidade está presenciando praticamente todos os dias. Ocorre que essa junção não é fácil de acontecer. Primeiro, é necessário que haja dados a serem coletados. Para que isso ocorra, deve ser possível buscar essas informações e armazená-las, o que demanda uma grande quantidade de memória computacional e uma infraestrutura robusta para a transmissão da informação. Até o fim dos anos 1990, o preço dos componentes desta infraestrutura - circuitos eletrônicos, cabos de fibra ótica e outros – era muito alto. Com o *boom* das empresas de internet, uma avalanche de investimentos em empresas de cabos óticos fez com que os preços para transmissão de dados despencassem (FRIEDMAN, 2014).

Uma vez gerado e transmitido o dado, é preciso filtrá-lo e analisá-lo. Em trinta minutos, por exemplo, um avião pode produzir mais informações que um homem consegue analisar em toda sua vida. Obviamente, o ser humano não consegue processar essa quantidade de dados apenas com sua capacidade cognitiva. Nem mesmo um computador comercial consegue processar tamanha gama de dados. O que permite essa filtragem é a capacidade de processamento de dados existente, que aumenta ano a ano. De acordo com a Lei de Moore, a cada 18 meses, aproximadamente, a capacidade computacional de um processador comum dobra (KUNER, CATE, *et al.*, 2012).

A grande virada ocorre quando surge o *Big Data,* que é existência de três variáveis simultaneamente: alta velocidade de processamento, grande volume de dados e ampla variedade de fontes de pesquisa. Como visto, o primeiro aumenta ano a ano, o segundo é possível graças à vasta infraestrutura disponível a preços baixos e o terceiro se tornou realidade com a Internet das Coisas (OLIVEIRA, 2018).

Some o *Big Data* à Inteligência Artificial e é possível utilizar os dados passados para fazer análise futuras, surgindo então o grande salto econômico. Com o uso de algoritmos complexos, os computadores aprendem a vasculhar dados, descartar o que não é útil, encontrar padrões e prever comportamentos póstumos. Mais ainda, as máquinas aprendem a tomar estas decisões sozinhas, sem que sejam programadas para isso, o que se chama de *machine learning.* Uma das

formas de se conseguir isso é por meio de *reinforcement learning*, quando se dá uma tarefa à máquina junto com uma base de dados robusta usada para treinamento. A máquina começa, no exemplo do jogo Go, a comparar cada jogada com o que é classificado na base de dados como movimentos bem-sucedidos. A cada interação, a máquina aprende o que a faz se aproximar do objetivo e, por meio de tentativas e erros infinitos, ela acaba criando jogadas melhores que as humanas. Quanto maior a capacidade de processamento de dados da máquina, mais rápido ela aprende (SAMPLE, 2017).

Um grande avanço ocorre quando a inteligência artificial consegue aprender mesmo sem um objetivo claro ou sem uma base de dados anterior, como ocorreu com o AlphaGo Zero. Neste caso, o sistema começou a rodar com uma rede neural que sabia apenas as regras básicas do jogo. A AI começa a jogar contra si mesma, combinando a rede neural com um poderoso algoritmo de busca. À medida em que vai jogando, a rede neural vai se ajustando e aprendendo a prever os movimentos. A cada interação, o sistema aprende um pouco mais, se tornando cada vez mais robusto. A AI fica limitada apenas à sua capacidade de processamento de dados e não mais ao conhecimento humano. Em quarenta dias, não apenas o AlphaGo Zero acumulou todo o conhecimento humano sobre o jogo como desenvolveu novos movimentos e estratégias até então desconhecidos (DEEPMIND, 2017).

Para Ram Charan, consultor de empresas como GE, KLM e *Bank of America*, dados são o petróleo do século XXI (CHARAN, 2017). Assim como há interesses privados, públicos e geopolíticos em torno do petróleo, também há disputas por trás dos dados. O valor comercial destas informações é quase inestimável; o Google, especializada em coleta de dados, em 2015 registrou lucro líquido de US$ 75 bilhões, sendo US$ 67,4 bilhões em propaganda. Ao cruzar diversos dados de seus usuários, a empresa consegue fazer com que os anúncios que chegam até eles sejam mais efetivos que qualquer outro tipo feito em outras mídias, trazendo mais retorno financeiro ao anunciante (BBC BRASIL, 2016).

Os alertas sobre os desdobramentos no futuro dessas novidades, no entanto, não são poucos. A ONU criou o Centro para Inteligência Artificial e Robótica em 2016 como forma de monitorar os avanços e alertar e conscientizar a população acerca dos riscos envolvidos (ONU, 2017). A ameaça de desemprego em massa é um dos problemas levantados não apenas pela organização, como por diversos

especialistas tanto em mercado de trabalho como em inteligência artificial ao redor do mundo. Estima-se que, apenas no Reino Unido, 30% dos postos de trabalho irão desaparecer em uma velocidade preocupante, de acordo com estudo realizado pela consultoria PwC. Quanto menos qualificação o posto exige, maior a probabilidade de no futuro ele ser preenchido por robôs, e quanto mais mão-de-obra desqualificada o país utiliza, mais vulnerável está sua sociedade (PWC, 2017).

O fim da privacidade é outro dos problemas a se enfrentar, uma vez que a tecnologia caminha para a interconexão de tudo (carro, geladeira, TV, computador, caminhões, robôs, câmeras de segurança, processos judiciais, etc.), gerando a coleta instantânea e maciça de dados, que serão – e já são – analisados pela inteligência artificial. Uma das “novidades” neste campo foi a criação de um algoritmo capaz de identificar, apenas por fotos, se uma pessoa é ou não homossexual, com uma taxa de acerto média de 85%. Em países onde a homossexualidade é crime, a tecnologia poderia ser usada para prender e até mesmo matar pessoas (WANG e KOSINSKI, 2017).

Percebe-se que a segurança desses dados é uma questão fundamental a ser tratada. Se por um lado, é possível imaginar uma verdadeira revolução graças ao uso destas informações - muitas das quais pessoais e sensíveis –, por outro há de se perguntar quem irá coletar esses dados, onde serão armazenados, quais empresas – ou governos – terão acesso a eles (BNDES, MCTIC, 2017). De acordo com relatório da UNCTAD, estabelecer confiança no ambiente virtual é vital para que as oportunidades que estão surgindo com a economia da informação sejam desenvolvidas em sua totalidade (UNCTAD, 2016)

Ao redor do mundo, a coleta e uso de dados tem despertado preocupação. Muitos países não regulam a matéria e há uma questão que adiciona ainda mais complexidade à discussão: o armazenamento de dados na nuvem (*cloud computing*) gera conflitos frequentes de jurisdição. Essa falta de segurança cria incertezas tanto nos usuários quanto nas empresas, o que tem o condão de diminuir o desenvolvimento econômico (UNCTAD, 2016).

Exemplos de mau uso de dados pessoais por empresas se proliferam. Em novembro de 2016, uma atualização de rotina no aplicativo Uber passou a forçar os usuários a compartilhar sua localização com a empresa mesmo após o usuário encerrar o uso do *software*. Para utilizar o aplicativo, ou o usuário concordava com

os termos de uso que permitiam o rastreamento, ou não poderia utilizá-lo. Na prática, a empresa estava rastreando todos os seus usuários por cinco minutos após o fim da corrida, coletando dados sobre o cotidiano da pessoa sem que ela pudesse discordar e muitas vezes sem que ao menos ela soubesse que isto estava acontecendo. Após fortes protestos de usuários e advogados, a empresa acabou com essa funcionalidade em agosto de 2017 (GIBBS, 2017).

Nos Estados Unidos, empresas especializadas em montar bancos de dados sobre pessoas para serem utilizados por empresas financeiras para cálculo de risco de crédito foram flagradas usando informações muito mais amplas que as divulgadas. Usuários tinham informações sensíveis como o consumo de álcool, orientação sexual e ocorrências policiais sendo utilizadas para definir seu risco de inadimplência sem que soubessem ou dessem permissão (OLIVEIRA, 2018).

Há ainda questões de segurança nacional, pois tudo que está conectado à rede pode ser atacado. Se toda a infraestrutura de um país está interligada, então toda ela pode ser *hackeada.* O mesmo vale para casas, órgãos do governo e empresas. Um exemplo de ataque ocorreu em 2017, com o *ransomware WannaCry,* utilizado para atacar centenas de milhares de computadores em mais de 150 países em apenas um final de semana, possibilitando que os dados de milhões de pessoas fossem roubados ou sequestrados de uma só vez (MICROSOFT, 2017). O ataque paralisou os Tribunais de Justiça de São Paulo, Espírito Santo, Minas Gerais, Roraima, Sergipe e todas as agências do INSS foram afetadas. No Reino Unido, hospitais públicos tiveram de ser fechados e cirurgias foram canceladas, pois os computadores tinham sido “sequestrados” e não era possível acessar prontuários. Dispositivos do mundo todo foram afetados e milhões de dados foram roubados (KASPERSKYLAB, 2017).

A segurança de dados é assunto tão importante que no final de 2016 foi criado no Brasil o Comando Conjunto de Defesa Cibernética, que reúne oficiais das três forças armadas nacionais. De acordo com o Ministério da Defesa, sua missão é planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e de capacitação no âmbito do Sistema Militar de Defesa Cibernética, sendo este seu órgão central, com o objetivo de assegurar o uso efetivo do espaço cibernético pelas Forças Armadas brasileiras e impedir ou dificultar sua utilização contra interesses da Defesa Nacional (MINISTÉRIO DA DEFESA, 2017).

Aprovada em dezembro de 2017, a Estratégia Nacional de Inteligência define o *Big Data* e as técnicas de análise de bancos de dados extensos (*analytics*) como uma das maiores oportunidades apara a atuação dos órgãos que compõem o Sistema Nacional de Inteligência (SISBIN), entre eles a Abin, a Polícia Federal, o Ministério da Justiça, entre outros. Por outro lado, no mesmo documento, ataques cibernéticos estão entre as principais ameaças ao Estado Democrático de Direito e à segurança nacional (BRASIL, 2017).

A possibilidade de roubo de dados é preocupante, mas outro aspecto da IoT também chama a atenção: a possibilidade da vigilância em massa de cidadãos por parte do governo. O site Wikileaks, especializado em vazamento de documentos governamentais confidenciais, divulgou 8.761 documentos da *Central Intelligence Agency* (CIA) que descrevem técnicas de *hacking* e vigilância de cidadãos, norte-americanos inclusive. Alguns dos documentos descrevem uma técnica para invadir aparelhos de televisão (TV) que possuam conexão com a internet e câmera de vídeo, dando ao órgão governamental acesso à toda atividade que se passar no cômodo onde se encontra o aparelho (MACASKILL, 2017).

Além da questão da privacidade, a evolução da inteligência artificial também vem sendo tratado com cuidado pela comunidade internacional. Em janeiro de 2017, uma série de especialistas assinaram uma carta aberta em que estabelecem padrões para a pesquisa sobre inteligência artificial, convocando os governantes do mundo todo a agirem para protegerem as sociedades. Pessoas como o físico Stephen Hawking, o cofundador da Apple Steve Wozniak, o criador da Microsoft Bill Gates, o CEO da Tesla Elon Musk, e pesquisadores de Harvard, Stanford, Berkeley, MIT, Cambridge, além de desenvolvedores de empresas como Google e Facebook, entre outros, assinam a carta e alertam que, deixadas à regulação pelo livre mercado, as novas tecnologias têm tudo para acabar com a raça humana (RUSSELL, DEWEY e TEGMARK, 2017).

Em uma segunda carta aberta, Elon Musk e Mustafa Suleyman, cofundador da *DeepMind*, em conjunto com outros 116 pesquisadores, solicitam que a ONU faça algo para banir as armas autônomas, como *drones,* tanques e metralhadoras que usam inteligência artificial e que já estão em desenvolvimento. De acordo com o documento, uma vez empregadas em larga escala, essas armas levarão a guerras

em escala jamais vista. Vale lembrar que estas armas não precisam de nenhuma interação com o homem para decidir quem matar (GIBBS, 2017).

A primeira carta traz uma série de questões a serem tratadas por diversos segmentos, inclusive pelo Direito. Responsabilidade civil e penal de veículos autônomos, políticas públicas para maximizar os bons resultados e mitigar riscos da AI, ética para profissionais da área da computação e engenharia, questões sobre privacidade e sobre armas autônomas estão entre as propostas. É preciso enfatizar que toda tecnologia pode ser usada para o bem ou para o mal, quem faz essa escolha é o homem. A questão que se levanta é que, com a singularidade se aproximando, teme-se que o homem não mais participará dessa decisão, pelo menos não como hoje (RUSSELL, DEWEY e TEGMARK, 2015).

A chegada da singularidade é praticamente consenso (KRUPAR, 2017). O termo, emprestado da física, descreve o momento em que situações tão extremas ocorrem que nenhuma equação consegue descrevê-las, o que acontece, por exemplo, nos buracos negros, onde a densidade infinita leva as equações existentes a gerar resultados absurdos. A singularidade na tecnológica designa o momento em que o próximo avanço tecnológico será tão grande, que tenderá ao infinito e deixará a capacidade cognitiva humana completamente obsoleta (KENSKI, 2016).

Se há um entendimento majoritário sobre a chegada da singularidade, o mesmo não pode ser dito sobre como enfrentar a revolução que o evento produzirá. Não se sabe nem mesmo quais serão seus desdobramentos, mas já se pode ter um vislumbre. No final de julho de 2017, o Facebook encerrou um projeto de AI depois que o robô começou a falar consigo mesmo em uma língua derivada do inglês, mas que apenas ele entendia. Ou seja, o robô, que havia sido desenhado para conversar com usuários, aprendeu uma forma mais “rápida” para estabelecer uma comunicação e criou uma nova língua, que nenhum engenheiro entendia. Antes que o robô começasse a se desviar demais do propósito para que foi construído, a equipe de inteligência artificial da empresa o desligou (KRUPAR, 2017).

O que se pode perceber logo de pronto é que a humanidade está diante de uma nova revolução, como afirma Manuel Castells. Novas situações surgirão das novas tecnologias em velocidade espantosa. Não se tem certeza sobre o que irá ocorrer, mas é unanime a percepção de que o final do século XXI em nada parecerá com seu início (CASTELLS, 1999).

Claramente, as tecnologias da comunicação e informação (TCI's), trazem muitos desafios ao sistema jurídico de qualquer país. Questões como a segurança de dados, responsabilidade civil e criminal pelo uso destes dados assim como pelos *softwar*es de inteligência artificial, conflitos de jurisdição entre países entre tantos outros temas, serão cada vez mais corriqueiros no dia a dia, e além disso, novas questões irão surgir com cada vez mais frequência e em velocidade cada vez maior. No caso do uso de dados, uma antiga questão se torna cada vez mais sensível: o equilíbrio entre privacidade e segurança. Para onde se olhe, novos desafios estão sendo propostos diariamente ao Direito. Neste contexto, é preciso entender quais são os atores envolvidos na eventual regulação – ou na defesa da não regulação – sobre temas relacionados às novas tecnologias, pois quais instituições darão respostas a essas questões é que moldará o futuro.

2 O CÓDIGO E SUA FORÇA REGULADORA

A tecnologia não é boa, não é ruim, mas nunca é neutra e sempre tem um aspecto regulatório embutido em si (KOOPS, 2007). Sempre foi assim e um exemplo muito claro disto é a fissão atômica, base tanto para a bomba nuclear como para reatores que geram eletricidade. A humanidade é composta por seres humanos diferentes entre si, que formam grupos de interesses mais ou menos coesos, cada qual defendendo seu ponto de vista (PZREWORSKI, 2010). Para alguns, produzir bombas atômicas é questão de segurança nacional, afinal, nada mais justo que um povo tenha condições de se defender de outros países que já tenham a tecnologia. Para outros, o simples fato de uma nação possuir tal arma já desestabiliza o sistema internacional por completo, então o desenvolvimento de qualquer tecnologia atômica deve ser evitada a todo custo. O Brasil, por exemplo, defende uma posição intermediária, em que o veto ao uso da energia nuclear com fins armamentistas não pode se tornar obstáculo para a pesquisa e seu desenvolvimento com fins pacíficos (MINISTÉRIO DAS RELAÇÕES EXTERIORES, 2018).

Desta forma, mais atenção é dada a cada posição a depender da relação entre os grupos de poder. Ora há maior restrição ao uso de energia nuclear, ora há menor, e assim acontece com todo e qualquer tema de interesse humano, em especial quando a discussão ocorre em democracias. Com as tecnologias da informação, acontece o mesmo. Diferentes grupos defendem diferentes posições, uns pela maior regulação outros pela menor (SCHULZ e DANKERT, 2016).

O que muda com as chamadas TIC’s (tecnologias da informação e comunicação) é o poder regulatório embutido nelas mesmas. Uma bomba atômica não tem a capacidade de forçar, por si só, nenhuma pessoa a fazer nada. Um povo pode jogar uma bomba sobre outro e ambos continuarem em guerra, sem que uma parte ceda à outra. Com *softwares* e algoritmos a situação é diferente. Comportamentos podem ser de fato impossibilitados ou forçados (KOOPS, 2007).

Ao se incorporar a criptografia no WhatsApp, por exemplo, o trabalho de investigação policial tradicional, por meio de interceptações de comunicação, é impossibilitado, alterando profundamente os meios de persecução penal (COSTA, 2016). Na telefonia tradicional, há a presunção de privacidade das conversas, que só pode ser violado mediante autorização judicial. Percebe-se que a privacidade é a

regra, mas há a possibilidade de uma exceção, qual seja, a escuta telefônica (BRASIL, 1996). Já no WhatsApp, a criptografia em sua forma atual impossibilita qualquer forma de interceptação de conversas, mesmo que o Estado a determine por meio de uma decisão judicial (COSTA, 2016). Ainda que haja meios alternativos para a realização de investigação policial, como a infiltração de agentes em grupos de conversas, um algoritmo criado por uma empresa privada alterou profundamente a forma como o Estado pode realizar seu trabalho policial (PARANÁ, 2017).

Exemplos de como a tecnologia consegue determinar comportamentos humanos abundam. Quando o Facebook cria filtros para eliminar conteúdo “danoso” do site, o que ocorre na prática é a censura feita por fórmulas matemáticas, resultando em excrescências como a proibição da publicação da famosa foto da garota correndo nua após ter sido atingida em um ataque com napalm na Guerra do Vietnã. O filtro, que deveria retirar do ar fotos de nudez infantil, acabou por censurar um dos registros fotográficos mais importantes da referida guerra (WONG, 2016).

Um outro exemplo chama ainda mais a atenção: *software*s estão sendo usados para fazer a dosimetria da pena em cortes norte-americanas. Em um recente caso concreto, *State vs. Loomis,* uma corte do Winsconsin, nos Estados Unidos, utilizou um algoritmo – desenvolvido por uma empresa privada – que mede a probabilidade de um indivíduo se tornar reincidente para calcular sua pena. Em 2013, Eric Loomis foi denunciado por cinco crimes relacionados a um tiroteio. O réu alegou inocência em três dos crimes e confessou os outros dois, de menor potencial ofensivo: não obedecer a ordem de parada de oficial de trânsito e dirigir sem licença (HARVARD LAW REVIEW, 2017).

Loomis foi condenado e, no momento de dosar sua pena, o Departamento de Correções de Winsconsin utilizou o *software Compas*, que determina a probabilidade de uma pessoa se tornar reincidente com base nos dados de sua ficha criminal e de uma entrevista que o condenado é obrigado a responder. Apenas o percentual de probabilidade de reincidência é entregue à Corte, já que o *software* é protegido por direitos autorais. Como exatamente o algoritmo chega ao percentual específico não é revelado nem às partes, nem à Corte (HARVARD LAW REVIEW, 2017).

No caso de Loomis, o *Compas* determinou que ele apresentava alto risco à sociedade e sua pena foi majorada. Em sede de recurso, a Suprema Corte de Winsconsin determinou que todo o procedimento era legal e que não havia nenhum

comprometimento da defesa, uma vez que o algoritmo utilizou apenas dados públicos para fazer sua avaliação. O caso criou muita polêmica nos Estados Unidos uma vez que uma das principais perguntas sobre o processo decisório do algoritmo não foi respondida: o sexo e a raça do réu tiveram algum peso na avaliação? Se tiveram, isso não seria errado, pois colocaria sobre uma pessoa o fardo do comportamento de outros? (HARVARD LAW REVIEW, 2017)

Estudos mostram que, nos Estados Unidos, a pena média dada a negros é maior que a média dada a brancos pelos mesmos crimes. Além disso, negros são considerados como de alto risco para a sociedade duas vezes mais que brancos, considerando apenas as pessoas que não reincidiram. Desta forma, ao utilizar uma base de dados impregnada de preconceitos, muito provavelmente algoritmos irão reproduzir estes pré-julgamentos e talvez legitimá-los, uma vez que os resultados são produzidos por máquinas, que são supostamente imparciais. Por outro lado, utilizados de forma criteriosa, algoritmos podem realmente retirar o preconceito humano da equação, ajudando o homem a tomar decisões mais justas (HARVARD LAW REVIEW, 2017).

No Brasil, há um caso interessante que ressurge a cada dois anos: a possibilidade de fraude nas urnas eletrônicas utilizadas nas eleições. Diego Aranha, professor da Unicamp, coordenou em 2012 um grupo de pesquisadores independentes convidados pelo governo para detectar possíveis falhas no *software* utilizados pelas urnas. De acordo com o pesquisador, o Tribunal Superior Eleitoral (TSE) impôs uma série de restrições sobre quais sistemas poderiam de fato ser investigados (a identificação biométrica, por exemplo, não pôde) e sobre quais pessoas podiam participar das auditorias, inclusive por questões de segurança nacional. Aranha foi um dos poucos pesquisadores independentes que participaram do processo e relata ter encontrado diversas falhas, como a possibilidade de descobrir a ordem e o horário de votação, potencialmente infringindo o sigilo de voto, além de ter encontrado o segredo de proteção do *software* inserido em seu código-fonte, o que facilita sobremaneira ataques contra o sistema (ARANHA, KARAM, *et al.*, 2014). Aranha, após participar destes testes, trabalha atualmente em conjunto com outros pesquisadores para desenvolver um *software* para urnas eletrônicas na Unicamp (PAYÃO, 2017).

Como este exemplo, outros se multiplicam. A Universidade MIT, dos Estados Unidos, conduz um estudo chamado de *Moral Machine*, sobre a responsabilidade de carros autônomos. Quando um humano provoca um acidente de trânsito, a forma de responsabilização é muito clara. O mesmo não ocorre com os carros autônomos. Em uma situação, por exemplo, em que o carro deve decidir se mata os ocupantes ou os pedestres – pois invariavelmente um dos dois fatos irá acontecer – percebe-se um claro dilema ético. A pesquisa mostra que as pessoas acreditam ser mais correto, em um nível hipotético, que carros autônomos privilegiem aqueles que seguem as leis. No entanto, quando perguntadas quais carros elas estariam mais propensas a comprar, as mesmas pessoas preferem aqueles que protegeriam elas mesmas (MIT, 2017).

Quando esta decisão deve ser tomada por uma pessoa, em geral não se questiona como ela foi feita. O indivíduo deve reagir em milésimos de segundos e decidir se mata outros ou desvia o carro, bate em um muro e potencialmente morre. Este tipo de conflito, onde é preciso escolher o menor de dois males, costuma ser resolvido mais por princípios e valores que pela lei em si. Neste caso, seria razoável exigir de um homem médio que ele se matasse para salvar outros? (SCHULZ e DANKERT, 2016)

Já quando uma máquina toma esse tipo de decisão, a situação é mais complexa. Ou a máquina tem uma base de dados que a leva a escolher determinada opção (matar os pedestres se eles estão atravessando no sinal vermelho, por exemplo) ou a máquina decide sozinha o que fazer, por meio de redes neurais (O'NEIL, 2016). Caso a máquina utilize uma base de dados, o ser humano é quem decidiu, *ex ante,* o que deverá ser feito. Quem deverá morrer entre a criança e o idoso, entre o pobre e o rico, entre o obeso e o magro, entre quem respeita as leis e quem não respeita. A máquina apenas obedece ao comando anteriormente dado, que é definido apenas pela empresa que desenvolve o algoritmo. No entanto, o *software* pode utilizar uma rede neural que é desenvolvida justamente para aprender sozinha, sem a interação com o homem, e fazer escolhas que nem mesmo os engenheiros desenvolvedores sabem como foram feitas (TASHEA, 2017) (O'NEIL, 2016).

Fica claro, então, que um poder muito grande de regulação do comportamento humano está nas mãos de empresas e de engenheiros que

desenham algoritmos amplamente utilizados pela humanidade. É importante frisar que, assim como toda invenção humana, as TIC's obedecem ao desenho elaborado por pessoas. O WhatsApp pode ou não ter criptografia ponta a ponta. O Facebook pode ou não eliminar conteúdo que julgar impróprio. A empresa pode muito bem ser forçada a esclarecer quais critérios foram utilizados para definir que certas pessoas têm maior chance de reincidir que outras. Por mais que haja uma sensação de um certo *determinismo tecnológico* na atualidade, ou seja, de que o avanço tecnológico é inevitável, na realidade, todo o desenvolvimento ocorrido até hoje decorre do esforço humano e, como tal, é sujeito à vontade do homem (LESSIG, 2006).

Se a Bolsa de Chicago anuncia que irá negociar contratos futuros de Bitcoin, a criptomoeda acumula valorização de 1.500% em onze meses, de janeiro a novembro de 2017 (TEMÓTEO, 2017). Já se a China decide restringir operações com esse tipo de ativo, a desvalorização bate os 70% em uma semana, retirando o equivalente a quase 2 trilhões de reais de circulação no mundo todo (RIZÉRIO, 2018). Há, portanto, uma decisão humana ocorrendo, seja para fomentar a tecnologia, seja para impedi-la (SCHULZ e DANKERT, 2016).

Sendo assim, é democrático que algumas centenas de pessoas definam a vida de milhões de outras sem nenhuma possibilidade de monitoramento? Atualmente, a esmagadora maioria dos algoritmos utilizados diariamente por populações inteiras é impossível de ser auditada. O primeiro obstáculo encontra-se nas leis que protegem direitos autorais e que autorizam as empresas a não revelarem seus segredos industriais e, portanto, seus códigos-fontes. É importante ressaltar que as essas leis são as mesmas que permitem, por outro lado, que as empresas cresçam e tragam desenvolvimento econômico. O equilíbrio a se encontrar aqui não é simples (O'NEIL, 2016).

Ocorre que, mesmo que os algoritmos fossem disponibilizados para o público, em vários casos não é possível fazer a chamada "engenharia reversa" para que o ser humano entenda exatamente como a máquina chegou àquela conclusão. Como exemplo, há o caso de uma professora de Washington, nos EUA, que foi demitida em razão de uma análise realizada por um *software*, criado especificamente para tal tarefa. Sarah Wysocki, mesmo tendo avaliações sempre muito positivas de colegas, pais e superiores, acabou tendo seu desempenho classificado pelo algoritmo como insatisfatório. Ao questionar a decisão junto à empresa, descobriu que nem mesmo

os engenheiros que fizeram o programa sabiam dizer quais dados tiveram maior peso para se chegar ao dito resultado. Havia a desconfiança de que as avaliações positivas que ela constantemente recebia tiveram bem menos impacto que outros dados colhidos, mas não era possível determinar isso com certeza (O'NEIL, 2016).

Cathy O'Neil, matemática formada em Harvard com extensa experiência em *Big Data* e algoritmos, afirma que grande parte dos *softwares* criados por pequenas e médias empresas tem um defeito grave, o chamado *feedback loop*, um processo que acaba por reforçar a aplicação de dados inconsistentes. Quanto mais o *software* "roda", mais ele cria distorções. Ela cita, em contraste, o Google, que consegue testar e monitorar centenas de variáveis diferentes, dado o alcance da empresa. Lá, os engenheiros podem mudar a cor dos anúncios, torná-los visíveis para dez milhões de pessoas, comparar os resultados com a cor anterior e concluir qual cor obteve mais visualizações. Por ser feito com centenas de milhares de pessoas e dados, esse *feeback* faz com que os algoritmos de busca do Google sejam constantemente afinados (O'NEIL, 2016).

Enfatize-se que, mesmo no Google, não é possível para quem está de fora entender como alguns dos algoritmos funcionam. Isso não é possível nem mesmo para os próprios engenheiros, em alguns casos. Especialistas em computação chamam esse efeito de *black box:* uma vez desenhado o código, não é possível saber o que sairá dele. Como uma verdadeira caixa-preta, o homem só controla a escrita do código. Quais dados serão utilizados, em qual ordem, com qual peso e qual será a conclusão são tarefas da máquina (O'NEIL, 2016).

Se o código – ou algoritmo – tem o poder de definir comportamentos, é natural em uma democracia assumir que cada pessoa que o utilize tenha direito de entender seu funcionamento. Também é natural concluir que cada pessoa tenha o direito de saber quais de seus dados estão sendo coletados, por quem, para serem entregues para qual empresa ou qual governo. Como estes dados estão sendo utilizados para, por exemplo, calcular seu risco de crédito ou o preço de sua apólice de seguro saúde. Mas não é isso que ocorre. Além de protegidos por leis que asseguram segredos comerciais e de não serem previsíveis, os algoritmos ainda são extremamente opacos (O'NEIL, 2016).

Uma questão levantada diante desta falta de transparência é que se a pessoa não concorda com a forma que a empresa trabalha, basta que ela não compre seu

produto. Se os filtros utilizados pelo Facebook parecem censura, basta não utilizar a rede social. Essa regulação feita pela sociedade tende a funcionar em vários casos, mas em outros, não. Muitas vezes, até que ela funcione, diversas pessoas já sofreram majoração de suas penas de forma indevida e países viram suas eleições manipuladas por robôs de redes sociais (FARIS, ROBERTS, *et al.*, 2017).

Com os algoritmos se tornando ferramentas cada vez mais poderosas para definir e limitar comportamentos humanos, é preciso fazer uma distinção entre eles e outra forma de regulação: as leis. A diferença fundamental entre estas e a tecnologia enquanto forças de regulação do comportamento humano é que as leis definem apenas como as pessoas *deveriam* se comportar, sendo sua força de aplicação apenas psicológica (KOOPS, 2007). As leis moldam o comportamento por meio de sanções, mas não impedem a ação. Caso uma pessoa mate a outra, ela será punida, mas em momento algum a lei restringe ou impede fisicamente o crime. A lei, portanto, não retira *a priori* a liberdade humana (LESSIG, 2006).

Já o código consegue efetivamente limitar o campo de atuação das pessoas, como uma espécie de cabresto. O comportamento humano pode ser completamente inviabilizado por um *software*, muito embora o código em si não tenha passado por nenhum processo ou crivo democrático (LESSIG, 2006). A lei que define que pessoas reincidentes devem receber penas mais longas foi aprovada pelo Parlamento e é, portanto, democrática. Enquanto isso, o programa de computador que calcula que uma pessoa tem mais chances que outra de reincidir sequer é transparente (KOOPS, 2007).

A maior função das leis é integrar a sociedade, mitigando potenciais conflitos e azeitando a máquina social. A única forma de sistemas de interação social não afundarem em conflitos e caos é por meio da adesão a um conjunto de normas legítimas passíveis de serem interpretadas e aplicadas. Além disso, um ordenamento jurídico traz certa estabilidade social ao reduzir a complexidade daquele conjunto de pessoas. As ações passam a ser “legais” ou “ilegais” e cria-se um meio para a solução de conflitos. Leis democraticamente aprovadas são, portanto, fundações para a sociedade ocidental moderna (SCHULZ e DANKERT, 2016).

Uma característica importante das leis é que elas possibilitam a interpretação, transformando-as conforme o tempo passa. A sociedade vai aos poucos, a cada

entendimento sobre suas normas, consolidando seu ordenamento. Interpretar as normas é parte do processo de construí-las. O código não permite isso. Há muito pouco espaço para correções feitas pela sociedade, a maior parte é feita pelos desenvolvedores. A diferença é bastante grande. Definido em outras palavras, o código tem o potencial de erodir a liberdade humana (SCHULZ e DANKERT, 2016).

Pzreworski lembra que a liberdade é mais que a base da democracia. Ela é *tudo*. A perda da liberdade seria um desastre. O cientista político faz uma distinção entre liberdade política e liberdade filosófica, como proposto anteriormente por Montesquieu. A última seria o exercício das vontades individuais. A primeira, a sensação de segurança trazida pela aplicação de leis, de forma que uns não temam aos outros. Esta liberdade só é possível quando o poder é dividido, do contrário, instala-se uma tirania. O grande desafio é equilibrar ambas, já que em geral, o aumento de uma implica a diminuição da outra (PZREWORSKI, 2010).

Como os *softwares* podem impor restrições, promover comportamentos e direcionar as pessoas, eles acabam assumindo funções de leis, mas sem obedecer a princípios democráticos. Desta forma, códigos escritos por empresas privadas acabam criando uma mudança na balança de poder, uma vez que a regulação passa a ser feita cada vez mais por atores privados, sem muita possibilidade, atualmente, de divisão deste poder por meio de instrumentos como a auditoria, por exemplo. Lawrence Lessig em 2006 alertava que isso poderia significar um determinismo tecnológico imposto por algumas pessoas, apenas aquelas que compusessem o corpo diretivo de empresas de tecnologia (SCHULZ e DANKERT, 2016).

O mesmo fato pode ser analisado sob diferente perspectiva: códigos podem transformar leis normativas em leis constitutivas. As primeiras são normas que deixam espaço para a liberdade pessoal: a lei pode determinar que se use cinto de segurança e a polícia pode multar quem não usar, mas ultimamente é o motorista quem decide se usa ou não o aparato. Leis constitutivas, no entanto, não permitem qualquer tipo de discricionariedade. Neste exemplo, um *software* pode simplesmente impedir que o motor do carro seja acionado enquanto o cinto de segurança não estiver afivelado (SCHULZ e DANKERT, 2016).

Desde sempre, há nas sociedades o equivalente físico dos algoritmos, o que Lessig chama de “arquitetura”. Caso uma prefeitura queira limitar o acesso de

caminhões em determinada rua da cidade, basta que seja construído um viaduto com altura baixa e, os veículos mais altos que ele, não conseguirão acessar tal rua. Se a mesma coisa for feita por atores privados sem autorização, há instituições com poder para forçar a demolição do viaduto. Desta forma, instituições legitimamente constituídas conseguem colocar em prática as leis aprovadas de forma democrática (SCHULZ e DANKERT, 2016).

O que os algoritmos têm feito é deslocar de certa forma o centro de poder para mais perto de empresas e para mais longe do setor público (SCHULZ e DANKERT, 2016). Um ponto central da discussão é a velocidade inversamente proporcional dos avanços tecnológicos em comparação com a capacidade das instituições democráticas, por exemplo, o Congresso Nacional, de conseguirem regular essas novas tecnologias. O sistema democrático pressupõe negociação entre diversos atores com diferentes interesses, o que demanda tempo (PZREWORSKI, 2010). Inovações, por outro lado, não esperam. Na realidade, várias das novas tecnologias surgem justamente por conta da falta de regulação de determinado mercado enquanto legisladores discutem sobre o assunto. Desta forma, o que ocorre na prática é que as inovações surgem e se consolidam antes mesmo que o Estado tenha iniciado a discussão sobre ela (COSTA NETO, 2018).

Há autores que afirmam que a democracia atual não consegue regular as novas tecnologias. Lawrence Lessig, por exemplo, defende que a melhor forma de regular as novas tecnologias é por meio delas mesmas. Muito embora as leis continuem sendo necessárias, para o professor o modo tradicional de criação de leis pelo processo democrático, por meio do Parlamento, é muito lento e não consegue dar respostas às necessidades muitas vezes urgentes que as novas tecnologias trazem. Para se proteger contra a erosão de privacidade, por exemplo, seria muito mais eficaz utilizar *software*s de proteção de dados que esperar que uma legislação sobre o tema seja criada e que ela efetivamente consiga limitar o problema (LESSIG, 2006).

Matthew Scherer, também da Faculdade de Direito de Harvard, chama a atenção para o fato de que métodos tradicionais de regulação, como responsabilidade civil, têm pouca eficácia para proteger a sociedade dos riscos trazidos pelas novas tecnologias. Essa dificuldade se deve principalmente à opacidade destas, ou seja, a dificuldade que agentes externos têm para identificar

suas falhas ou ameaças e à sua difusão, uma vez que pessoas em várias jurisdições diferentes trabalham simultaneamente no desenvolvimento da mesma tecnologia (SCHERER, 2016).

Já Schulz, da Universidade de Hamburgo, afirma que os códigos, uma vez que assumem o papel de leis, devem passar por crivos democráticos assim como estas, ainda mais considerando a força auto executória dos algoritmos. O autor lembra que a regulação privada acontece há décadas, mas que ultimamente ela tem aumentado graças à ampliação do uso de *softwares* no dia-a-dia e que ela tende a crescer mais ainda (SCHULZ e DANKERT, 2016).

Se há muita discussão sobre *como* regular as TIC's, há também muito embate sobre *até que ponto* elas devem ser reguladas. Como trazido anteriormente, leis que asseguram o segredo empresarial, ao mesmo tempo em que tornam os algoritmos extremamente opacos, permitem avanços tecnológicos que muito beneficiam toda a humanidade. Países como a Suécia interferem demasiadamente na vida privada do cidadão, regulando comportamentos nos mínimos detalhes. Outros, como os EUA, entendem que o Estado deve interferir o mínimo possível no mercado (PZREWORSKI, 2010). O equilíbrio é delicado e é preciso levar em conta o poder que os consumidores têm para fazer uma empresa, ideia ou algoritmo emplacar ou não. Basta lembrar do Orkut, que já foi a maior rede social do mundo e hoje não passa de lembrança (SCHULZ e DANKERT, 2016).

De uma forma ou de outra, o cerne da questão é o debate em si. Da forma como a maioria dos algoritmos é desenhada atualmente, não há espaço para debates. Empresas usam o fato de o indivíduo ser alcóolatra para cobrar mais juros em seu empréstimo e isso não é nem autorizado, nem divulgado, sequer a pessoa sabe como esse dado foi parar na empresa. Estados usam algoritmos para demitir servidores e estes não conseguem descobrir nem quais dados foram utilizados. No modelo atual, falta muita transparência, um dos pilares da democracia, que possibilita com que as pessoas consigam fazer decisões informadas (PZREWORSKI, 2010).

É por meio desta transparência que os indivíduos conseguem definir até que ponto querem que o Estado interfira no cotidiano. A população de certa cidade pode escolher que aplicativos de carona podem funcionar sem nenhuma interferência estatal. A mesma população pode escolher justamente o contrário, caso descubra

que os aplicativos estão usando a cor da pele do usuário como métrica para precificar corridas, por exemplo. Caso opte por mais restrições, isso deve ser feito por normas aprovadas pelos poderes estatais legitimamente constituídos. Não há outro caminho para a democracia a não ser por meio da escolha da maioria (PZREWORSKI, 2010).

Vale lembrar que não existe “democracia”. O que se tem são diferentes democracias, no plural, cada uma com suas particularidades, seus limites e suas características. Não existem dois regimes democráticos idênticos em lugar nenhum do mundo. Igualdade, participação, representação e liberdade variam conforme a profundidade, maturidade ou consistência de uma democracia (PZREWORSKI, 2010).

Desta forma, é importante que a sociedade tenha formas de se expressar e definir o que deseja, seja por meio de leis elaboradas por instituições democráticas, seja pela força reguladora que os consumidores têm. Pzreworski, no entanto, pondera que, apenas onde o livre mercado de fato funciona, é que a sociedade consegue limitar a atuação de empresas da forma como entender ser melhor para ela. Ou seja, apenas onde o mercado funcione com concorrência de fato, sem oligopólios significativos, ao mesmo tempo em que o Estado interfira na economia para garantir essa livre concorrência, é que a sociedade consegue ter poder de limitar a atuação de empresas pela via do consumo (PZREWORSKI, 2010).

Assim, por mais que haja diferentes tipos e níveis de democracias, alguns elementos básicos devem estar presentes para que se fale em poder do povo de fato. Aqui, vale a pena retomar um pouco o nascimento do regime político para melhor contextualizar o propósito do trabalho. Desde o seu surgimento, a democracia já passou por diversas mudanças de conceito. Os *founding fathers*, líderes políticos norte-americanos que escreveram e assinaram a Constituição de 1776 dos Estados Unidos, criaram um sistema que limitava o poder central, no intuito de se retirar o poder da aristocracia representante da metrópole britânica e concedê-lo às colônias locais. De forma alguma o intuito originário era o governo do povo, tanto que muitos estados do país continuaram a proibir o voto de afrodescendentes até meados do século XX. Na França não foi diferente. A Revolução Francesa de 1789 não objetivava dar o poder ao povo. Ao contrário, a

burguesia temia um governo composto por ele. O intuito era substituir a aristocracia como detentora de poder (PZREWORSKI, 2010).

O que hoje se entende por democracia é algo muito diferente do imaginado pelos *founding fathers* ou pela burguesia francesa. É também extremamente distinto do modelo grego clássico, de atuação direta, onde todos os cidadãos tinham a certeza de que governariam Atenas, nem que fosse por um dia. Ainda hoje há aqueles que defendem que o sistema democrático deve ser direto, com a atuação efetiva de todo o povo. No entanto, em países populosos como na atualidade, a democracia direta é simplesmente impossível, assim como indesejável (PZREWORSKI, 2010).

A forma representativa de governo é a melhor opção, dado que a atuação direta é inviável, e a melhor forma de se escolher representantes é pelo voto. Por mais carregadas de defeitos que sejam a democracia e suas eleições, ainda assim, são a melhor e menos custosa forma de se colocar pessoas para governar outras. É por meio do voto que se elegem parlamentares, principais responsáveis por criar leis. É, então, por meio do Parlamento e de instituições democraticamente estabelecidas que se consolida um Estado democrático. Não é possível falar em democracia se a grande maioria das leis e normas são feitas por atores privados, sem espaço para conferências (KOOPS, 2007). Também não é possível falar em democracia quando a liberdade é erodida, por quem quer que seja (PZREWORSKI, 2010).

Diante de tantos desafios, onde um lado da balança parece anular o outro, talvez a melhor – e mais democrática solução – para o problema da falta de transparência dos algoritmos seja o estabelecimento de formas de governança dos mesmos, de modo que a população tenha acesso ao seu funcionamento, sem que haja perigo demasiado de roubo de informações sigilosas (SCHULZ e DANKERT, 2016).

3 A REGULAÇÃO NO BRASIL

Para compreender o impacto das novas tecnologias na regulação social, é necessário analisar como se dá a aprovação de leis sobre o tema no país. Neste ponto, dada a vastidão de assuntos abrangidos pelo termo “novas tecnologias”, optou-se por avaliar a legislação sobre privacidade, uma vez que esta permeia quase todo o tema. Desde redes sociais a aplicativos de compartilhamento, praticamente todos se valem do uso de dados pessoais, como já vastamente explorado neste trabalho.

Desde pelo menos o século XIX, a privacidade é tema de discussão no Direito ocidental. Em 1890, no artigo *The right to Privacy* publicado na revista *Harvard Law Review,* Samuel Warren e Louis Brandeis estabelecem um marco para a discussão sobre o tema. À época, a fotografia instantânea, que passou a ilustrar jornais, era novidade e havia o sentimento de que representava séria ameaça à vida privada de todos. Bastava a pessoa sair de casa para que estivesse sujeita a ser fotografada e ter sua imagem publicada em jornais de grande circulação. Os autores do artigo defendiam o *right to be left alone,* ou seja, o direito de “ser deixado em paz”, como forma de proteger a privacidade de cada um (FONTES, 2018).

O intuito do estudo era formular um princípio que resguardasse a intimidade das pessoas contra a invasão da imprensa. Surgiu então o direito à privacidade, que nada mais era que conferir a cada um a total disponibilidade para decidir como suas emoções e pensamentos podem ser transmitidos a outros. Assim, o indivíduo conserva em seu poder a capacidade de manter reservado o assunto que não quer ver divulgado. O direito à privacidade garante, então, proteção aos assuntos mais íntimos, imateriais e emocionais que são parte da formação da própria subjetividade da pessoa. O princípio se sustenta, ainda, no fato de que, na tradição anglo-saxã, ninguém pode ser forçado a dizer nada, a não ser na condição de testemunha e, ainda que decida falar fora deste contexto, a pessoa sempre deve ter autonomia para definir o alcance de suas palavras (FONTES, 2018).

Em entendimento mais recente, no contexto das décadas de 1960 e 70, Malcolm Warner e Michael Stone propuseram que o direito à privacidade também diz respeito a garantir que as informações geradas por uma pessoa sejam utilizadas exatamente da maneira que pretendeu, não podendo as mesmas serem

empregadas contra o próprio indivíduo que as produzir. Percebe-se que o conceito adquire diferentes nuances ao longo do tempo e de acordo com quem os interpreta. De qualquer forma, há um consenso majoritário de que a privacidade é entendida como direito humano e, portanto, fundamental (FONTES, 2018).

Mesmo com tamanha importância, a privacidade, ou o uso de dados pessoais não encontra proteção direta no Brasil. No ordenamento jurídico pátrio não há uma norma geral que trate especificamente sobre proteção de dados pessoais. É possível encontrar regulação sobre o tema em diferentes diplomas, desde a Constituição Federal até leis ordinárias, no entanto, em todas elas, a proteção conferida é indireta. Os principais diplomas que tratam do tema são a Carta Magna, a Lei 9.507/1997 que regula o *Habeas Data,* o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei 12.414/2011), a Lei de Acesso à Informação (Lei 12.527/2011) e o Marco Civil da Internet (Lei 12.965/2014).

No Brasil, há o entendimento doutrinário de que os dados pessoais são parte da personalidade do indivíduo e devem, portanto, ter a mesma proteção que outros direitos correlatos, como o direito ao nome, por exemplo. O Código Civil traz em seus Artigos 11 a 21 os direitos de personalidade e embute ali as suas características fundamentais: a generalidade (são concedidos a todos), a oposição absoluta ou *erga omnes* e a extrapatrimonialidade, ou seja, a impossibilidade de ser avaliado economicamente. Estas características também estão presentes nos dados pessoais, o que os tornam verdadeiros direitos personalíssimos, que dizem respeito à dignidade da pessoa humana (LINDOSO, 2018).

O Inciso X, do Artigo 5º, da Constituição Federal determina que “são invioláveis a intimidade e a vida privada, a honra e a imagem das pessoas”, o que também confere um certo grau de proteção às informações pessoais, desde que sejam entendidas como parte da intimidade e da vida privada do ser humano. O Inciso XII do mesmo Artigo traz que “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”. Isto também confere proteção indireta aos dados pessoais, em especial contra avanços do Estado sobre o indivíduo. Além disso, o Inciso LXXII do mesmo Artigo 5º assegura a concessão do

Habeas Data para garantir o conhecimento ou retificação de dados constantes de registros públicos (BRASIL, 1988).

Essa proteção que a Constituição confere à intimidade das pessoas protege indiretamente os dados gerados por elas, mas não traz nada a respeito de consentimento, transparência e outros tópicos importantes sobre o tema. O *habeas data,* regulamentado pela Lei 9.507 de 1997, diz respeito apenas a dados que estejam em registro ou banco públicos, não contemplando os que estejam sob domínio privado, o que torna sua eficácia limitada. O sigilo de dados ser inviolável também não tem muita eficácia prática quando se trata de dados pessoais colhidos na internet, com autorização do usuário, mas que são utilizados para fins diferentes daqueles autorizados pelo seu dono (BRUM DA SILVA e LEAL DA SILVA, 2016).

O Código de Defesa do Consumidor (CDC), embora tenha sido o primeiro diploma no ordenamento brasileiro a trazer efetivamente a proteção de dados, o fez apenas no caso de concessão de crédito nas relações de consumo. O CDC e também o Código Civil tratam ainda do contrato de adesão, aquele elaborado unilateralmente por uma das partes, sem que o aderente tenha possibilidade de realizar qualquer mudança. Em geral, os termos de uso de plataformas que coletam dados pessoais são verdadeiros contratos de adesão que demandam muito tempo de leitura. Os termos de uso do Instagram formam um documento com quarenta páginas, enquanto os do Facebook preencheriam trinta e seis. Já se discute se estes tipos de contrato, que definem o uso dos dados pessoais dos usuários, são abusivos ou não (VIOLA, 2017).

Outro diploma que trata de dados pessoais é a Lei Complementar 105/2001, exclusivamente sobre sigilo bancário e financeiro. Em 2011, houve a aprovação da Lei 12.414, que trata do cadastro de crédito positivo, primeiro dispositivo a trazer o conceito de consentimento: para figurar o cadastro, a pessoa deveria consentir e os dados só poderiam ser utilizados para aquela finalidade específica (VIOLA, 2017). Com a nova lei, inverteu-se a lógica anterior de que apenas informações desabonadoras sobre os clientes, que tratavam apenas da inadimplência, poderiam ser divulgadas. Abriu-se espaço no Brasil para a criação de bancos de dados que alimentam sistemas de pontuação para concessão de crédito (OLIVEIRA, 2018).

A referida lei ainda veda a coleta de dados excessivos para a formação do cadastro individual, evitando assim que dados potencialmente discriminatórios sejam

utilizados para a avaliação do risco de crédito. Também fica restrito o uso de dados que apresentem juízo de valor sobre as pessoas. O artigo 3º da Lei 12.414 define os conceitos do que seriam dados objetivos, dados que apresentam juízo de valor, informações sensíveis e excessivas. No entanto, tudo isto se aplica apenas aos bancos de dados com informações sobre adimplemento (OLIVEIRA, 2018).

A chamada Lei de Acesso à Informação (Lei 12.527/11), foi a primeira a definir o que era “informação pessoal” e dar tratamento diferenciado a informações sensíveis ou sigilosas em relação a outros tipos de dados. O Marco Civil da Internet (Lei 12.965/2014), trata sobre o tema da privacidade sem se aprofundar. Ele estabelece a proteção de dados e da privacidade como princípios norteadores da internet no Brasil, assegura a inviolabilidade da intimidade dos usuários e a necessidade de consentimento qualificado para a coleta de dados, mas não passa disso (VIOLA, 2017).

A legislação existente no Brasil não trata de diversos assuntos relacionados aos dados pessoais, como a venda dessas informações por empresas, a anonimização, a responsabilização dos agentes que coletam e tratam esses dados em caso de vazamento ou roubo, entre outros pontos que são fundamentais tanto para a proteção dos usuários quanto para o estabelecimento de empresas de tecnologia no Brasil. Para o Ministro do Superior Tribunal de Justiça Ricardo Villas-Bôas Cueva, é urgente a aprovação de uma lei que trate de proteção de dados pessoais, inclusive para fomentar o desenvolvimento econômico do país (CANÁRIO, 2017).

Neste sentido, tramitam nas casas parlamentares três projetos de lei com objetivo de regular a questão da privacidade na internet no país: o PL 5.276/12, o PL 4.060/12, ambos com tramitação inicial da Câmara dos Deputados e o PLS 330/13, que teve início no Senado Federal. O primeiro foi de iniciativa do Poder Executivo, por meio do Ministério da Justiça, que realizou consultas públicas online e é, dentro todos os projetos de lei que tramitam no Congresso Nacional, o mais completo e preciso, de acordo com diferentes pesquisadores (OLIVEIRA, 2018) (VIOLA, 2017).

O PL 5.276/12 foi apensado ao PL 4.060/12, de iniciativa do Deputado Federal Milton Monti de São Paulo, e tanto estes quanto o PLS 330/13 tiveram intensa movimentação nas Casas Legislativas. Em outubro de 2017, o PLS chegou a entrar na pauta de votação da Comissão de Assuntos Econômicos, mas foram

apresentadas subemendas que obstaram a votação. O PLS é de autoria do Senador Antonio Carlos Valadares de Sergipe (SENADO FEDERAL, 2018) (CÂMARA DOS DEPUTADOS, 2018).

O PLS 330/13, embora mais completo que o PL 4.060/12, carece de maior especificidade. No entanto, a movimentação legislativa parece ser no sentido de incorporar a este projeto o texto do PL 5.276. Uma questão política fez com que o PLS 330 tramitasse com mais rapidez que o PL 5.276: este último foi de iniciativa do Ministério da Justiça e foi apresentada à Câmara dos Deputados no último dia de governo da ex-presidente Dilma Rousseff, um dia antes da votação de seu *impeachment*. Parece haver nas casas legislativas uma certa resistência em levá-lo adiante por este motivo, mas está se trazendo para o corpo do PLS 330 a maior parte do texto do PL 5.276 (VIOLA, 2017) (LEMOS, 2017).

O PL 4.060/12, dos três em tramitação acima citados, é o mais impreciso por não definir uma série de questões fundamentais. O texto trata de disposições gerais, firma alguns princípios, traz requisitos necessários para o tratamento de dados, trata de forma superficial em dois parágrafos sobre direitos do titular dos dados e fala sobre fiscalização e sanções, também de forma genérica. Critica-se o projeto por ser incompleto, deficiente e genérico e por não tratar do tema na profundidade necessária (VIOLA, 2017).

Já o PL 5.276 se aprofunda bastante no tema e traz proteção adequada à coleta de dados. No modelo do Marco Civil, o projeto é muito mais principiológico que normativo, no intuito de não o deixar envelhecer rápido, uma necessidade premente quando se trata de regular novas tecnologias. O texto traz definições claras sobre o que são dados pessoais, dado sensíveis, bancos de dados, entre outros que são de suma importância para a devida proteção dos usuários. Traz também requisitos para a coleta e tratamento de dados, como a implementação de governança que permita aos usuários o acesso a que dados estão sendo coletados e para onde eles estão indo. Fala sobre a transferência internacional de dados, dos direitos do titular, dos agentes responsáveis pela coleta e da fiscalização (VIOLA, 2017).

A exposição de motivos do PL 5.276/2016 traz o projeto como forma de garantir o “livre desenvolvimento da personalidade e da dignidade da pessoa natural”. Ressalta que foram seis meses de consultas públicas promovidas pelo

Ministério da Justiça, com mais de mil contribuições. O texto da lei foi elaborado pelo Ministério em conjunto com a Universidade Federal de Minas Gerais e o Núcleo de Informação e Coordenação do Ponto BR (Nic.Br). De acordo com o texto, o intuito do projeto é “assegurar ao cidadão o controle e a titularidade sobre suas informações pessoais, com fundamento na inviolabilidade da intimidade e da vida privada”, além de reforçar que a coleta de dados é importante para o desenvolvimento de novos conhecimentos, mas é também potencial fonte de riscos para a privacidade (CÂMARA DOS DEPUTADOS, 2016).

A justificativa para o projeto ainda chama a atenção para o fato de o Brasil ter sido o principal articulador, junto com a Alemanha, para a aprovação da resolução “Direito à privacidade na era digital” pela ONU. O documento apoia fortemente o direito à privacidade e solicita que todos os países tomem providências para coibir as violações neste sentido, seja por atores privados ou públicos. A aprovação do documento se deu no contexto do “caso Snowden”, em que o ex-funcionário da *NSA (National Security Agency)* revelou que os EUA mantinham um programa de espionagem que mirou a então Presidente Dilma Rousseff e a Chanceler alemã Angela Merkel (ONU, 2013)

O PL 5.276/16 lembra ainda que 109 países possuem normas sobre proteção de dados e 90 têm alguma autoridade pública especializada no assunto. Ressalta ainda o caráter transnacional da coleta de dados e o perigo potencial no tratamento de dados sensíveis, que podem levar à discriminação. A conclusão do documento é que a regulação sobre o tema se faz necessária tanto para proteger o titular dos dados quanto para estimular seu uso de forma segura, transparente e com base no princípio da boa-fé (CÂMARA DOS DEPUTADOS, 2016).

Uma das críticas sobre o PL 5.276 é que ele dispõe sobre o aparato fiscalizatório, mas sem ser específico o suficiente. Ele prevê a criação de um órgão com participação da sociedade civil, academia, setor privado, mas com ampla maioria de membros do governo, que é um dos agentes que coleta e armazena dados. Há um claro conflito de interesses na forma como a lei define a composição do órgão e também não há definições claras sobre sanções a serem aplicadas em caso de descumprimento da lei (VIOLA, 2017).

Por óbvio, não é possível adiantar qual dos três projetos será aprovado, sendo também possível que nenhum deles o seja. O que se observa é que existe

um diálogo democrático ocorrendo, como demonstram as diversas audiências públicas que têm sido feitas, com representantes da sociedade civil, do governo e da academia sempre presentes. Já participaram destes encontros representantes de associações de indústrias de *software*s e de eletrônicos, professores de diversas universidades nacionais e internacionais, promotores de justiça, prepostos de institutos de pesquisa sobre internet e inovação, associações de empresas de marketing, delegados federais, diretores de empresas de tecnologia, entre outros (CÂMARA DOS DEPUTADOS, 2018) (SENADO FEDERAL, 2018).

Além das discussões no âmbito legislativo, está em andamento um estudo sobre *IoT* financiado majoritariamente pelo BNDES. Atuam no projeto, além do Banco, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD), a consultoria McKinsey e o escritório Pereira, Neto e Macedo Advogados. O projeto se divide em três fases: levantamento do mercado de IoT no mundo, definição dos setores prioritários da economia brasileira para receber os investimentos necessários para o desenvolvimento de IoT e a formulação de ações voltadas para acelerar a implantação do mercado de IoT no país. Em diversos momentos destas etapas, estão previstas consultas públicas sobre o tema. (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, 2017).

Como a tramitação das leis sobre privacidade de dados e do estudo sobre IoT se dão de forma paralela e com vários atores semelhantes, espera-se que um seja complementação do outro. O Plano Nacional de IoT tratará de ações para o desenvolvimento de tecnologias que usam a internet no dia a dia das pessoas e das empresas. E irá além, tratando também de temas como segurança de dados, regulação, privacidade e capacitação de recursos humanos (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, 2017).

O que se percebe é que a discussão sobre o tema está ocorrendo de forma democrática, no âmbito do Congresso Nacional, absorvido pela instituição legitimamente constituída para tanto. Um ponto crucial, no entanto, é o que está acontecendo enquanto a lei não é aprovada. Neste ínterim, o judiciário tem se tornado cada vez mais atuante, quase que substituindo o legislativo em sua função. Dois casos demostram tal situação: a presença da Uber e uma decisão do Superior Tribunal de Justiça sobre a Lei 12.414/11. No primeiro caso, a atuação do judiciário

é que garante a permanência da empresa em diversas cidades brasileiras. A Uber é internacionalmente conhecida por atuar burlando a lei, se aproveitando da pressão social e de decisões monocráticas para forçar os poderes Executivos locais a aprovar leis que beneficiem a empresa (COSTA NETO, 2018).

Em que pese a sociedade pressionar o legislativo para que a empresa seja regularizada, o que reveste o processo de legitimidade democrática até certo ponto, surge a dúvida se a empresa não estaria apenas se aproveitando do apoio para se estabelecer como monopólio, o que no final vai contra a vontade social que, no caso do Brasil, seria pelo fim do monopólio dos taxistas. Além disso, é notório que a empresa burla os meios democráticos de discussão para garantir sua atuação, se valendo de liminares concedidas pelo Judiciário para tanto. A empresa, que tem um caixa robusto, tem condições financeiras de ingressas na justiça, enquanto os próprios motoristas ou outras empresas concorrentes não têm, provocando distorções no mercado (COSTA NETO, 2018).

Em todas as vinte cidades onde houve a regulação do transporte por aplicativos, a discussão se limitou à concorrência entre taxistas e motoristas de aplicativos. Em nenhuma delas houve propostas para modernizar o serviço de taxi nem discussões sobre mobilidade urbana, sustentabilidade ou qualquer coisa neste sentido. As leis aprovadas se limitaram a impor barreiras aos aplicativos como forma de igualar a concorrência com os taxis, impedindo a livre concorrência e deixando de lado a vontade e bem-estar dos cidadãos. Percebe-se, nestes casos que, muito embora as leis tenham sido aprovadas conforme manda o rito democrático, elas possuem pouca legitimidade (COSTA NETO, 2018).

O segundo exemplo de como o Judiciário tem substituído o Legislativo na regulação de novas tecnologias é a decisão do Superior Tribunal de Justiça sobre a Lei 12.414/11. A Súmula 550, aprovada em 2015, dispensa o consentimento do usuário para que seus dados constem do cadastro positivo de empresas de *credit scoring*, muito embora a referida lei, em seu parágrafo 4º, seja explícita ao afirmar que a inscrição no cadastro só pode ser feita mediante consentimento informado. São dois entendimentos completamente contrários e a decisão do Tribunal muda a própria essência da lei (COSTA NETO, 2018).

Ocorre, também, que nem toda discussão que ocorre no Congresso Nacional sobre o tema é de grande valia. A Senadora Vanessa Grazziotin, do PCdoB do

Amazonas, propôs um projeto de lei (PL 347/2016) que determina que a inclusão de pessoas em grupos, páginas e comunidades virtuais só pode ser feita com consentimento prévio do usuário. Ou seja, antes de adicionar os netos nos grupos de família, as avós terão, primeiro, que solicitar o consentimento informado dos mesmos. Caso a pessoa seja adicionada a grupos sem ter dado o consentimento "livre, específico, inequívoco e informado", a empresa desenvolvedora do aplicativo – Facebook, WhatsApp, Telegram, entre outros – poderá responder por danos morais. E caberá à empresa provar que houve o consentimento, invertendo-se o ônus da prova. O projeto de lei já foi aprovado pela Comissão de Constituição, Justiça e Cidadania e seguiu para ser votado na Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (SENADO FEDERAL, 2018).

Diante do exposto, pode-se extrair algumas características da regulação das novas tecnologias no Brasil, que se aplicam diretamente aos dados pessoais. De fato, há uma discussão democrática sendo feita em uma instituição legitimamente constituída para tanto, em âmbito federal, muito embora nem toda proposta levada adiante seja de qualidade. Nos estados e municípios, pontos fundamentais têm ficado de fora do debate, na maioria das vezes. Além disso, enquanto a regulação é feita em âmbito federal, há forte judicialização da demanda, que acaba por distorcer o mercado antes que a lei seja aprovada. Talvez seja o caso de o Brasil olhar para fora e buscar exemplos de como regular a questão sem limar a livre iniciativa.

4 GOVERNANÇA

Atualmente, no sistema internacional há basicamente dois tipos gerais de regulação sobre o tema: o norte-americano e o europeu. O primeiro consiste em uma série de normas feitas por cada setor social, sem regulação federal ou geral. Nos EUA, por exemplo, o setor de educação, de saúde e o bancário têm, cada um, normas próprias sobre privacidade de dados. Já a União Europeia trata o tema com regulações gerais, que se aplicam a todos os casos. A tendência mundial é seguir a forma normativa europeia, uma vez que as leis deste continente determinam que transações comerciais, cooperações jurídicas e várias outras formas de intercâmbio só podem ocorrer se os países adotarem certas medidas definidas pela União Europeia. Como exemplo, o Brasil tem uma série de barreiras na cooperação jurídica com o continente justamente por não ter uma regulação geral sobre privacidade de dados (VIOLA, 2017).

Em ambos os casos, uma parte fundamental da regulação passa pela chamada governança. Grupos de governança têm diferentes propósitos e estruturas mais ou menos complexas. Possuem desde objetivos mais simples, como definir conceitos, até os mais complexos, como complementar a atuação de uma agência governamental ou ajudar na elaboração de leis. Em todos os casos, os grupos de governança ajudam a unificar a linguagem entre os atores envolvidos, facilitando a comunicação e colocando todos os participantes na mesma página (GASSER, BUDISH e MYERS WEST, 2015).

Estes grupos podem ter um papel central na definição e implantação de normas e conceitua-los se torna cada dia mais difícil. Um grande exemplo é o que ocorre na internet, que forma um verdadeiro ecossistema, onde incontáveis atores têm papel fundamental para que ela seja como a conhecemos. Para que um computador se conecte a outro, é preciso gerenciar os endereços de IP, de forma que cada máquina tenha uma identidade única. A rede física de cabeamento ótico, que transmite os dados entre esses computadores, é gerenciada por diferentes empresas e, em alguns países, pelo governo central, que precisam conversar entre si para que os dados trafeguem entre as nações. Os domínios precisam ser unificados no mundo todo, de forma que haja apenas uma internet - ou seja, o endereço www.google.com deve levar ao site da empresa Google,

independentemente de onde o internauta esteja. Estes são apenas alguns exemplos do que envolve a internet e cada decisão acerca de cada um desses tópicos envolve milhares de pessoas em dezenas de países diferentes que, de forma coordenada, trabalham nos chamados grupos de governança, de forma que a internet seja uma só e não várias. O principal grupo de governança da internet é o ICANN, que tem grande proximidade com o governo norteamericano, uma vez que nasceu no Departamento de Defesa do país (ICANN, 2018).

Outros grupos de governança atuam de forma mais local ou regional. O INCB (*Israel National Cyber Bureau)*, por exemplo, reúne diversos atores apenas daquele país para garantir a execução de leis locais sobre *cyber* segurança. Alguns grupos pretendem, ainda, se tornar alternativas para as instituições estabelecidas, como é o caso dos desenvolvedores do Bitcoin, que atuam totalmente fora das instituições e pretendem substituir as moedas nacionais, o que demonstra que nem sempre esses grupos se propõem a ser democráticos, no sentido de promover discussões na sociedade (GASSER, BUDISH e MYERS WEST, 2015).

Um caso emblemático no Brasil foi o a formatação do Marco Civil da Internet que envolveu a sociedade civil, os Poderes Executivo e Legislativo federais, a academia, a comunidade técnica e a iniciativa privada, de forma colaborativa. Utilizando a própria internet, o Ministério da Justiça iniciou consultas públicas que duraram dezoito meses e tiveram grande participação popular. Vários encontros pessoais realizados com os atores já citados ocorreram ao longo do processo. Após redigir um documento inicial, que contava com colaborações elaboradas tanto nas consultas quanto nas reuniões, o projeto foi submetido ao Congresso, que ainda o alterou, antes de aprova-lo. Nas casas legislativas ainda foram realizadas mais consultas públicas e mais reuniões. Foram sete anos desde o início das discussões até que a lei fosse aprovada. O processo foi bastante transparente, mesmo tendo sido tão complexo e envolvendo diversas forças antagônicas (GASSER, BUDISH e MYERS WEST, 2015). Pode-se afirmar que toda a aprovação da lei foi extremamente democrática, levando-se em conta os parâmetros definidos por Pzreworski, quais sejam, a transparência, a participação e a igualdade entre os envolvidos (PZREWORSKI, 2010).

A tabela abaixo, retirada de um estudo feito em Harvard, demonstra que cada ator definiu claramente sua posição sobre cada assunto em discussão, assim como nenhum deles saiu vitorioso em todos os quesitos.

***Tabela 1**: posição de cada ator envolvido versus legislação aprovada, por tema.*

Issues/Actors	Net Neutrality	Highly Enhanced Privacy	Safe Harbor for Speech	Data Retention	Forced data Localization	Safe Harbor for Copyright	Express Removal for Revenge Porn
Telcos	Against	Against	Neutral	Neutral	Neutral	Neutral	Neutral
Civil Society	For	For	For	Against	Against	For	Against
Global Internet Companies	Neutral	Against	For	Neutral	Against	For	Neutral
Brazilian Internet Companies	For	Against	For	Against	Against	Against	Neutral
Broadcast sector	For	For	For	Neutral	Neutral	Against	Neutral
Government (Executive branch)	For	Neutral	Neutral	For	For	Neutral	For
Law enforcement lawyers/ Federal Police	Neutral	Against	Against	For	For	Against	For
Passed legislation	Passed	Passed	Passed	Passed	Rejected	Rejected	Passed

Fonte: GASSER, U.; BUDISH, R.; MYERS WEST, S. Multistakeholder as Governance Groups: Observations from Case Studies. Cambridge. 2015.

Percebe-se que houve transparência nas posições defendidas, os atores foram agrupados conforme sua atuação e a lei foi aprovada pela instituição legitimidade constituída para tanto. Todos os envolvidos tiveram suas demandas ouvidas e nenhum deles conseguiu ter peso suficiente para pesar demais a balança para seu lado. A discussão foi feita de forma democrática e, de fato, refletiu não apenas a vontade popular, entendida como coletividade, como a de todos os grupos de interesse, entendidos como individualizações. A legislação aprovada é um equilíbrio aceito por todos, onde nenhum envolvido teve todas as suas posições aceitas ou rejeitadas (GASSER, BUDISH e MYERS WEST, 2015). Exatamente o que Adam Przeworski define como decisão democrática (PZREWORSKI, 2010).

A atuação de grupos de governança no processo legislativo, então, não conflita *per si,* com a democracia. No entanto, para que funcione, é necessário que haja muitos indivíduos envolvidos, com representação de diversas posições, que haja espaço para negociações intensas, muito debate e que haja organização. O processo que utiliza o conceito de *multistakeholders* não garante que a lei aprovada será melhor, mas, no caso do Marco Civil, deu mais transparência ao processo legislativo (GASSER, BUDISH e MYERS WEST, 2015).

No caso brasileiro, o que se pode afirmar que contribuiu positivamente para o resultado final da legislação foram seis fatores: instituições governamentais de fato estavam interessadas na participação pública; a comunidade tinha muito interesse no tópico em discussão; um grupo de pesquisadores com vontade genuína de contribuir com suas experiências, influenciando o debate; uma *interface* que permitiu construir uma narrativa comum para políticos e cidadãos, de forma que não houvesse ruídos demais nas discussões; políticos que conseguiram identificar os pontos chave dos debates e transforma-los em um texto coerente; e recursos financeiros suficientes para que o processo avançasse (GASSER, BUDISH e MYERS WEST, 2015).

Não há um modelo definido de como um grupo de governança deva ser ou trabalhar de forma a maximizar as chances de sucesso. No entanto, alguns pontos surgiram no estudo realizado pelo *Berkman Center for Internet & Society* da Universidade de Harvard. Os mais bem-sucedidos são aqueles que se mantêm atentos durante todo o processo ao contexto histórico e cultural da sociedade, aos potenciais grupos de apoio e às oportunidades de barganha relacionadas a inclusão, transparência e *accountability.* Os grupos que se mantiveram atentos a estes fatores e como eles mudam ao longo do tempo foram aqueles que, no estudo, tiveram os melhores resultados. Ou seja, aqueles mais aptos a entender o contexto cultural do local onde operam são os mais bem-sucedidos (GASSER, BUDISH e MYERS WEST, 2015).

Não há um consenso sobre qual a melhor forma para se regular as novas tecnologias (SCHULZ e DANKERT, 2016). Como já trazido anteriormente pelo trabalho, há os que defendem que a melhor regulação de uma TIC é aquela feita por ela mesma (LESSIG, 2006). Outros entendem que qualquer coisa feita fora das instituições estatais tem um vício de legitimidade (O'NEIL, 2016). Há um posicionamento intermediário que estabelece que é o meio termo entre as duas coisas que melhor atenderá ao propósito (SCHULZ e DANKERT, 2016).

O estabelecimento de grupos de governança como uma forma auxiliar à discussão parlamentar parece ser a saída mais interessante, levando-se em conta que a democracia implica necessariamente em debate. Se os conflitos não são absorvidos por instituições legitimamente constituídas, o que se tem a prevalência de uma posição em detrimento de outra baseado em outros poderes que não o da

argumentação, como por exemplo, a capacidade financeira de uma empresa (PZREWORSKI, 2010).

É preciso ter em mente que grupos de governança podem ter inúmeros objetivos diferentes, não apenas discutir políticas públicas. Eles podem servir, por exemplo, para ajudar a implementar a política definida, juntamente com agências reguladoras (SCHERER, 2016). Há nos projetos de lei sobre privacidade dados em tramitação no Congresso a previsão de constituição de um órgão formado por entes estatais e privados para supervisionar a aplicação da lei, nos moldes de um grupo de governança.

Se por um lado, Przeworski afirma que a democracia direta não funciona e nem é desejável sua aplicação, por outro também não é interessante que o poder regulador seja demasiadamente aplicado por empresas e atores privados. O estabelecimento de grupos de governança parece ser um caminho viável entre as duas coisas, desde que eles de fato consigam compreender e exprimir o contexto social em que estão inseridos (PZREWORSKI, 2010) (SCHULZ e DANKERT, 2016) (GASSER, BUDISH e MYERS WEST, 2015).

CONCLUSÃO

Inteligência artificial, *Big Data, analytics, machine learning,* redes neurais, *internet of things*. Termos há pouco tempo inexistentes e que hoje estão diariamente estampados nos jornais, nos artigos científicos, nas conversas pessoais, no dia-a-dia. As tecnologias da informação e comunicação se tornam cada vez mais onipresentes. Mais da metade da população mundial é conectada à internet e, com o crescimento da *IoT,* esse número tende a crescer. São bilhões de pessoas interagindo todos os dias na rede, produzindo dados sobre suas preferências, seus amores, seus dessabores, suas paixões. São bilhões de pessoas utilizando, direta ou indiretamente, essas novas tecnologias da informação. São bilhões de pessoas, de alguma forma, sendo utilizadas pelas TICs.

Desde que o homem criou a primeira ferramenta e conseguiu dominar o fogo, a tecnologia e seus desdobramentos fazem parte do dia-a-dia da humanidade. Desde sempre, novas descobertas são a glória e o fracasso humano. O mesmo instrumento de ferro utilizado para plantar alimentos, também é usado para matar pessoas. O avião, que encurtou distâncias e aproximou pessoas, pode ser utilizado para jogar bombas em civis. Toda tecnologia sempre foi e sempre será utilizada para o bem e para o mal. Com as TICs não seria diferente.

Verdadeiras revoluções são esperadas graças ao uso de inteligência artificial, *big data, analytics*, entre outros. É plausível esperar que *todos* os campos do conhecimento sejam afetados de alguma forma. Medicina, psicologia, engenharia, biologia, enfim, tudo o que se conhece será impactado pelas novas tecnologias, uma vez que *a humanidade* em si será atingida. Direito, sociologia e ciências políticas também passarão por transformações, como não poderia deixar de ser.

Não é possível prever como será o mundo daqui cem anos, muito embora seja plausível afirmar que em nada se parecerá com o que existe hoje. As cidades, os carros, os tratamentos médicos, as formas de locomoção, tudo isso e muito mais será diferente. Cem anos atrás, em 1918, ainda se acreditava que doenças se propagavam pelo miasma. Carros eram tão pouco populares que a arquitetura das cidades era diferente, com ruas mais estreitas e mais espaços para pedestres. Muito mudou nos últimos cem anos e a humanidade tem fortes razões para acreditar que muito mais irá mudar nos próximos cem.

Se todas as áreas do conhecimento humano serão afetadas pelas novas tecnologias e elas podem ser usadas tanto para construir quanto para destruir, é preciso que se assegure a máxima utilização benéfica das mesmas. Mesmo assim, a humanidade errará e, tentando fazer o bem, pode ser que o resultado seja só o mal, conforme demonstra a história. Antes da eclosão da Primeira Guerra Mundial havia uma sensação generalizada, talvez muito parecida com a atual, de que os avanços tecnológicos seriam de alguma forma a panaceia para todos os problemas humanos. Acreditava-se que o progresso era infinito e constante. A Grande Guerra tratou de mostrar que não é bem assim.

Toda tecnologia criada é fruto da invenção humana e, como tal, é intrinsecamente suscetível a falhas. O homem erra e, portanto, a tecnologia erra. A melhor forma de se proteger as pessoas destes erros é, primeiramente, admitir a possibilidade de falhas – o que não raro é rechaçado por entusiastas das TICs. O pensamento é lógico: se há risco de falha, é necessário que se monitore, que haja checagem, que se tenha transparência. Do contrário, se a tecnologia é infalível, não há razão para seu controle. É muito recorrente no mundo das *startups* e da *disrupção* encontrar pessoas que creem piamente na infalibilidade das tecnologias e aqui está o perigo. É preciso que as sociedades se conscientizem da necessidade de transparência e *accountability* para que os algoritmos tragam os resultados tão promissores que se espera.

Em um mundo onde *tudo* traz consigo algum algoritmo, a força regulatória das fórmulas matemáticas passa a ser gigantesca. Se toda atividade do homem que vive em sociedade passará, de forma direta ou indireta, por *softwares*, nada mais justo que cada um tenha a possibilidade, se desejar, de entender como isso funciona. Mesmo quem não esteja conectado à internet, de forma alguma, em algum momento, terá sua vida impactada por algoritmos. Pode ser no dia em que for buscar um empréstimo, quando *softwares* de análise de risco de crédito serão utilizados para calcular os juros a se pagar. Pode ser no dia em que o preço do alimento cair em função da maior produtividade no campo. Pode ser, ainda, em um futuro não muito distante, quando algum conhecido for morto por um policial robô que apresentou um *bug.*

Conectados ou não, a todos interessa o assunto. Saber o que são algoritmos, como funcionam, como fazem seus cálculos, como chegam a determinados

resultados. Se as pessoas não puderem saber isso, não existirá mais democracia. Um mundo onde a vida é regulada por algoritmos feitos por empresas privadas – ou governos – sem a possibilidade de conferência pelo povo nada mais é que uma tirania, onde poucos governam muitos, sem que haja a menor satisfação ou responsabilização pelos atos cometidos.

Ultimamente, quem deve decidir o alcance das novas tecnologias e seus usos lícitos ou ilícitos é o povo, por meio de seus governantes eleitos ou ainda por meio da força de mercado. Por óbvio, para que isso seja minimamente legítimo e funcional, é preciso que se haja um sistema político de fato representativo e uma economia de livro mercado. Desta forma, é possível garantir que o sistema de freios e contrapesos funcionará sempre que exageros forem criados.

Não se espera, no entanto, que cada cidadão fique de vigília o tempo todo, sempre acompanhando *tudo* relacionado a novas tecnologias. A solução mais viável é aquela que mescla pessoas bem informadas sobre os assuntos que mais lhe afetam fazendo pressão pelo que desejam, em um mercado livre e concorrencial, que permita que empresas nasçam, inovem e também que quebrem. Além disso, é preciso que as instituições sejam legitimamente constituídas, que o Parlamento de fato represente a vontade da maioria e que ele seja apto a absorver as demandas sociais. Por fim, a formação de grupos de governança, com pessoas especializadas e capazes de auditar as TICs, é fundamental para que o ciclo virtuoso se complete.

No Brasil, a regulação tem sido feita, até hoje, de forma mista. O Parlamento trabalhou em consonância com a população e com grupos de interesse na aprovação do Marco Civil da Internet. A população se fez presente de forma direta, por consultas públicas e de forma indireta, por meio dos grupos de pressão, grupos de interesse ou grupos de governança. A lei foi discutida no âmbito do Parlamento, aprovada após intensa negociação. Por mais que tenha demorado, obedeceu a todos os trâmites democráticos. No entanto, nem toda aprovação de leis passa pelo mesmo procedimento e não raro as normas aprovadas simplesmente não se conectam com políticas públicas voltadas para a inovação.

Quando se fala em controle pelo mercado, não são as raras as distorções geradas no país. Decisões judiciais diferentes em cada município, em cada Estado, geram deformidades no mercado, seja forçando, seja barrando a atuação de empresas. Por outro lado, a pesada burocracia também acaba por não permitir que

a pressão popular funcione de forma adequada. O Estado e as empresas ainda precisam melhorar muito no quesito transparência e os cidadãos precisam se educar para entender certas questões, como por exemplo a exposição de privacidade nas redes sociais.

Sopesando todo o pesquisado neste trabalho, percebe-se que é de extrema importância que se assegure a liberdade individual das pessoas frente ao poder regulatório dos algoritmos, seja quando utilizados pelo Estado, seja quando utilizados pela iniciativa privada. E é garantindo a transparência que se garante a liberdade. É preciso que se atente ao meio e não ao fim da jornada. De nada adianta tentar prever os resultados. O que a humanidade deve fazer é engendrar seus melhores esforços para assegurar a forma democrática de se escolher as coisas, com seus freios e contrapesos. Invariavelmente, as sociedades errarão. Tecnologias serão, mais de uma vez, utilizadas com efeitos nefastos. No entanto, o que mais importa é que a possibilidade de controle democrático e a liberdade nunca sejam afastadas.

REFERÊNCIAS

AGROSMART. *Para alimentar o mundo, é preciso trazer inovação para a agricultura*, 2017. Disponivel em: <https://www.agrosmart.com.br/blog/alimentar-o-mundo-trazer-inovacao-para-agricultura/>. Acesso em: 37 março 2018.

ARANHA, D. et al. *(In)segurança do voto eletrônico no Brasil*, 2014. Disponivel em: <http://www.kas.de/wf/doc/13775-1442-5-30.pdf>. Acesso em: 27 março 2018.

ASSOCIAÇÃO BRASILEIRA DE GO. *Site*, outubro 2017. Disponivel em: <https://abrago.org/>. Acesso em: 20 dezembro 2017.

BBC BRASIL. *Como o Google Ganha dinheiro?* BBC Brasil, 2016. Disponivel em: <http://www.bbc.com/portuguese/noticias/2016/03/160329_google_dinheiro_fn>. Acesso em: 27 março 2018.

BNDES, MCTIC. IoT: *Relatório do Plano de Ação*, Brasília, 2017. Disponivel em: <https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-plano-de-acao-produto-8-alterado.pdf?MOD=AJPERES&CVID=m0jDUok>. Acesso em: 27 março 2018.

BONNEFON, J.-F.; SHARIFF, A.; RAHWAN, I. *The social dilemma of autonomous vehicles*. Science, 352, 2016. Disponivel em: <http://science.sciencemag.org/content/352/6293/1573.full>.

BRASIL. *Constituição da República Federativa do Brasil*, Brasília, 1988. Disponivel em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>.

BRASIL. *Lei 9.296, de 24 de julho 1996*, julho 1996. Disponivel em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso em: 27 março 2018.

BRASIL. *Estratégia Nacional de Inteligência*, Brasília, 15 dezembro 2017. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/Dsn/Dsn14503.htm>. Acesso em: 27 março 2018.

BRUM DA SILVA, L.; LEAL DA SILVA, R. *A proteção jurídica de dados pessoais na internet*: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil., 2016. Disponivel em: <http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65>. Acesso em: 27 março 2018.

CÂMARA DOS DEPUTADOS. *Projeto de Lei 5.276/2016*, 2016. Disponivel em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=DEB418EB573EA373E107BAC0BA0F2DCB.proposicoesWebExterno2?codteor=1457459&filename=PL+5276/2016>. Acesso em: 27 março 2018.

CÂMARA DOS DEPUTADOS. *Atividade Legislativa*: PL 4.060/12, 2018. Disponivel em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066&ord=1>. Acesso em: 27 março 2018.

CANÁRIO, P. *Brasil precisa de lei sobre proteção de dados pessoais, diz Villas-Bôas Cueva*. Conjur, Agosto 2017. Disponivel em: <https://www.conjur.com.br/2017-ago-15/brasil-lei-protecao-dados-pessoais-cueva>. Acesso em: 27 março 2018.

CASTELLS, M. *A sociedade em Rede*. 6a edição. ed. São Paulo: Del Rey, v. I, 1999.

CHARAN, R. *Estratégias para vencer em tempos de incerteza*. São Paulo: [s.n.]. novembro 2017.

CHIEN, A.; KARAMCHETI, V. *Moore's Law*: The First Ending and a New Beginning. Computer, v. 46, n. 12, 2013.

CISCO. *Cisco connected mass transit*, 2017. Disponivel em: <https://www.cisco.com/c/dam/en_us/solutions/industries/docs/sdmts-casestudy.pdf>. Acesso em: 27 março 2018.

COSTA NETO, A. F. D. Entre os novos comportamentos sociais e as velhas ferramentas regulatórias: uma análise sobre a trajetória da regulação do Uber nas capitais brasileiras. In: FERNANDES, R. V. D. C.; COSTA, H. A.; DE CARVALHO, A. G. P. *Tecnologia jurídica e direito digital*: I Congresso Internacional de Direito e Tecnologia. Belo Horizonte: Fórum, 2018.

COSTA, C. *Quatro coisas que mudam com a criptografia no WhatsApp*. BBC Brasil, 2016. Disponivel em: <http://www.bbc.com/portuguese/noticias/2016/04/160406_whatsapp_criptografia_cc>. Acesso em: 27 março 2018.

DEANGELIS, S. *Practical Artificial Intelligence Is Already Changing the World*. Wired, 2017. Disponivel em: <http://insights.wired.com/profiles/blogs/practical-artificial-intelligence-is-changing-the-world>. Acesso em: 27 março 2018.

DEEPMIND. *AlphaGo Zero:* Learning from scratch, 2017. Disponivel em: <https://deepmind.com/blog/alphago-zero-learning-scratch/>. Acesso em: 27 março 2018.

ERICSSON. *Ericsson Mobility Report*, Estocolmo, 2016. Disponivel em: <https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf>. Acesso em: 27 março 2018.

FARIS, R. et al. *Partisanship, Propaganda, and Disinformation*: Online Media and the 2016 U.S. Presidential Election. Berkman Klein Center, 2017. Disponivel em: <https://cyber.harvard.edu/publications/2017/08/mediacloud>. Acesso em: 27 março 2018.

FLECK, I. *Apoio a governo militar no Brasil é maior que média global*, diz pesquisa. Folha de São Paulo, 2017. Disponivel em: <http://www1.folha.uol.com.br/poder/2017/10/1927419-parcela-que-apoia-governo-militar-no-brasil-e-maior-que-media-diz-pesquisa.shtml>.

FONTES, V. B. A incorporação dos direitos de privacidade na internet no sistema jurídico brasileiro. In: FERNANDES, R. V. D. C.; COSTA, H. A.; DE CARVALHO, A. G. P. *Tecnologia jurídica e direito digital:* I Congresso Internacional de Direito e Tecnologia. Belo Horizonte: Fórum, 2018.

FRIEDMAN, T. L. *O mundo é plano*: o mundo globalizado no séxulo XXI. São Paulo: Companhia das Letras, 2014.

GASSER, U.; BUDISH, R.; MYERS WEST, S. *Multistakeholder as Governance Groups*: Observations from Case Studies. Berkman Center Research, Cambridge, 2015. Disponivel em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549270>. Acesso em: 27 março 2018.

GIBBS, S. *Elon Musk leads 116 experts calling for outright ban of killer robots*. The Guardian, 2017. Disponivel em: <https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war>.

GIBBS, S. *Uber pulls U-turn on controversial tracking of users after trip has ended*. The Guardian, Agosto 2017. Disponivel em: <https://www.theguardian.com/technology/2017/aug/29/uber-u-turn-tracking-users-after-trip-ended-app-user-privacy-new-ceo>. Acesso em: 27 março 2018.

GOODMAN, M. *Future Crimes*. São Paulo: HSM Editora, 2015.

HARVARD LAW REVIEW. *State v. Loomis*, Boston, 2017. Disponivel em: <https://harvardlawreview.org/2017/03/state-v-loomis/>. Acesso em: 27 março 2018.

IBM. *6 Benefits of IoT for Hospitals and Healthcare*, 2017. Disponivel em: <https://www.ibm.com/blogs/internet-of-things/6-benefits-of-iot-for-healthcare/>. Acesso em: 27 março 2018.

ICANN. ICANN. *Site*, 2018. Disponivel em: <https://www.icann.org/>. Acesso em: 27 março 2018.

INTERNET SOCIETY. *Internet Governance*, 2017. Disponivel em: <http://www.internetsociety.org/what-we-do/internet-issues/internet-governance>.

KASPERSKYLAB. *WannaCry: o que você precisa saber*, 2017. Disponivel em: <https://www.kaspersky.com.br/blog/wannacry-for-b2b/7324/>. Acesso em: 27 março 2018.

KENSKI, R. *Singularidade*. Superinteressante, São Paulo, 2016. Disponivel em: <https://super.abril.com.br/ciencia/singularidade/>. Acesso em: 27 março 2018.

KOOPS, B.-J. *Criteria for Normative Technology*. Tilburg University, 2007. Disponivel em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=%201071745>. Acesso em: 27 março 2018.

KRUPAR, F. *A match made in hell? Distributed Ledgers and Artificial Intelligence*, 2017. Disponivel em: <https://feed.itsrio.org/a-match-made-in-hell-distributed-ledgers-and-artificial-intelligence-aa38b2641daf>. Acesso em: 27 março 2018.

KUNER, C. et al. *The challenge of 'big data' for data protection*. International Data Privacy Law, Oxford, v. 2, n. 2, 2012.

LEMOS, R. *Curso sobre Marco Civil da Internet*: histórico. [S.l.]: [s.n.]. 2017.

LESSIG, L. *The Constitution of Code*: Limitations on Choice-based Critiques of Cyberspace Regulation. CommonLaw Conspectus, 1997.

LESSIG, L. *Code version 2.0*. [S.l.]: Amazon, 2006.

LINDOSO, M. C. B. Conflitos no uso da tecnologia do Big Data: violação de privacidade e discriminação pelo processamento de dados. In: FERNANDES, R. V. D. C.; COSTA, H. A.; DE CARVALHO, A. G. P. *Tecnologia jurídica e direito digital*: I Congresso Internacional de Direito e Tecnologia. Belo Horizonte: Fórum, 2018.

MACASKILL, E. *WikiLeaks publishes 'biggest ever leak of secret CIA documents'*. The Guardian, Março 2017. Disponivel em: <https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance>. Acesso em: 27 março 2018.

MICROSOFT. Schneider *Electric harnesses the sun to power remote Nigerian schools and clinics*, 2017. Disponivel em: <https://blogs.microsoft.com/transform/feature/schneider-electric-harnesses-the-sun-to-power-remote-nigerian-schools-and-clinics/#sm.0001wu94xi1fpecu11569oi7t4m36>. Acesso em: 27 março 2018.

MICROSOFT. *The need for urgent collective action to keep people safe online*: Lessons from last week's cyberattack, maio 2017. Disponivel em: <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.000003khb86r9mehlpiuxwgjhzrel>. Acesso em: 5 maio 2017.

MICROSOFT. *Veja como a Microsoft IoT apoia a agricultura sustentável*, 2017. Disponivel em: <https://www.microsoft.com/pt-br/internet-of-things>. Acesso em: 27 março 2018.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. *MCTIC anuncia diretrizes do Plano Nacional de Internet das Coisas nos próximos dias*, fevereiro 2017. Disponivel em: <http://www.mcti.gov.br/noticia/-/asset_publisher/epbV0pr6eIS0/content/mctic-anuncia-diretrizes-do-plano-nacional-de-internet-das-coisas-nos-proximos-dias>. Acesso em: 5 maio 2017.

MINISTÉRIO DA DEFESA. *Comando Conjunto na Defesa Cibernética*, 2017. Disponivel em: <http://www.defesa.gov.br/noticias/30417-comando-conjunto-na-defesa-cibernetica>. Acesso em: 27 março 2018.

MINISTÉRIO DAS RELAÇÕES EXTERIORES. *Desarmamento nuclear e não proliferação*, 2018. Disponivel em: <http://www.itamaraty.gov.br/pt-BR/politica-externa/paz-e-seguranca-internacionais/146-desarmamento-nuclear-e-nao-proliferacao-nuclear>. Acesso em: 27 março 2018.

MIT. *Moral Machine*. Site, 2017. Disponivel em: <http://moralmachine.mit.edu/>. Acesso em: 20 dezembro 2017.

MUKHERJEE, S. *A.I. versus M.D*. The New Yorker, New York, 3 abril 2017. Disponivel em: <https://www.newyorker.com/magazine/2017/04/03/ai-versus-md>. Acesso em: 27 março 2018.

NETMUNDIAL. *Global Multistakeholder Meeting on the Future of Internet Governance*, 2014. Disponivel em: <http://netmundial.br/about/>. Acesso em: 2018.

OLIVEIRA, C. E. G. D. Credit Scoring e Big Data no regime jurídico brasileiro. In: FERNANDES, R. V. D. C.; COSTA, A.; CARVALHO, A. G. P. D. *Tecnologia jurídica e direito digital*: I Congresso Internacional de Direito e Tecnologia. Belo Horizonte: Fórum, 2018.

O'NEIL, C. *Weapons of Math Destruction*. New York: Broadway Books, 2016.

ONU. *Assembleia Geral da ONU aprova resolução de Brasil e Alemanha sobre direito à privacidade*, 2013. Disponivel em: <https://nacoesunidas.org/assembleia-geral-da-onu-aprova-resolucao-de-brasil-e-alemanha-sobre-direito-a-privacidade/>. Acesso em: 27 março 2018.

ONU. *UNICRI Centre for Artificial Intelligence and Robotics*, 2017. Disponivel em: <http://www.unicri.it/in_focus/on/UNICRI_Centre_Artificial_Robotics>. Acesso em: 27 março 2018.

PARANÁ. *Ação Penal n. 504686367.2016.4.04.7000/PR*, 2017. Disponivel em: <http://www.mpf.mp.br/pr/sala-de-imprensa/docs/SENTENAHASHTAGINTEGRA.pdf.pdf>. Acesso em: 27 março 2018.

PAYÃO, F. *Urnas eletrônicas: falhas, vulnerabilidades e fraudes do mesário*. Tecmundo, 2017. Disponivel em: <https://www.tecmundo.com.br/seguranca/122152-urnas-eletronicas-falhas-vulnerabilidades-fraudes-mesario.htm>. Acesso em: 20 dezembro 2017.

PEW RESEARCH CENTER. *Globally, Broad Support for Representative and Direct Democracy*. New York. 2017.

PWC. *Will robots steal our jobs? The potential impact of automation on the UK and other major economies*, Londres, 2017. Disponivel em: <https://www.pwc.co.uk/economic-services/ukeo/pwcukeo-section-4-automation-march-2017-v2.pdf>. Acesso em: 27 março 2018.

PZREWORSKI, A. *Democracy and the limits of self-government*. New York: Cambridge University Press, 2010.

RIZÉRIO, L. *Bitcoin*: a enxurrada de más notícias que leva à nova queda livre e perda de US$ 550 bi das criptomoedas. Infomoney, 2018. Disponivel em: <http://www.infomoney.com.br/mercados/bitcoin/noticia/7251944/bitcoin-enxurrada-mas-noticias-que-leva-nova-queda-livre-perda>. Acesso em: 27 março 2018.

RUSSELL, S.; DEWEY, D.; TEGMARK, M. *Research priorities for robust and beneficial artificial intelligence*. Future of Life Institute, 2017. Disponivel em: <https://futureoflife.org/ai-open-letter/>. Acesso em: 27 março 2018.

SAMPLE, I. *'It's able to create knowledge itself':* Google unveils AI that learns on its own. The Guardian, Londres, 2017. Disponivel em: <https://www.theguardian.com/science/2017/oct/18/its-able-to-create-knowledge-itself-google-unveils-ai-learns-all-on-its-own>. Acesso em: 27 março 2018.

SAMPLE, I. T*he algorithms that are already changing your life*. The Guardian, 2017. Disponivel em: <https://www.theguardian.com/science/2017/nov/03/from-health-to-crimefighting-ai-has-brought-us-to-the-threshold-of-a-new-era>. Acesso em: 27 março 2018.

SCHERER, M. U. *Regulating artificial intelligence systems:* risks, challenges, competencies, and strategies. Harvard Journal of Law & Technology, 2016. Disponivel em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2609777>. Acesso em: 27 março 2018.

SCHULZ, W.; DANKERT, K. *'Governance by Things' as a challenge to regulation by law*. Internet Policy Review, 5, n. 2, 30 junho 2016. Disponivel em: <https://policyreview.info/articles/analysis/governance-things-challenge-regulation-law>. Acesso em: 27 março 2018.

SENADO FEDERAL. *Atividade Legislativa: Projeto de Lei do Senado n. 330 de 2013*, 2018. Disponivel em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 27 março 2018.

SENADO FEDERAL. *Inclusão em grupos virtuais deverá ter consentimento prévio de internauta*, fevereiro 2018. Disponivel em: <https://www12.senado.leg.br/noticias/materias/2018/02/07/inclusao-em-grupos-virtuais-devera-ter-consentimento-previo-de-internauta>. Acesso em: 27 março 2018.

SHANAHAN, M. *The Technological Singularity*. [S.l.]: MIT Press, 2016.

SOCIEDADE NACIONAL DA AGRICULTURA. *Sistema ajuda a reduzir gasto de água na irrigação*, 2014. Disponivel em: <http://sna.agr.br/embrapa-desenvolve-sistema-para-reduzir-gasto-de-agua-na-irrigacao/>. Acesso em: 27 março 2018.

TASHEA, J. *Courts are using AI to sentence criminals. That must stop now*. Wired, 2017. Disponivel em: <https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/>. Acesso em: 20 dezembro 2017.

TEMÓTEO, A. *Bitcoin causa euforia e preocupação; valorização é de 1.500% em 2017*. Correio Braziliense, 2017. Disponivel em: <http://www.correiobraziliense.com.br/app/noticia/economia/2017/12/12/internas_economia,647223/o-que-e-bitcoin.shtml>. Acesso em: 27 março 2018.

TERRA. *Fog Computing é o novo paradigma para a Internet das Coisas, diz Cisco,* 2017. Disponivel em: <http://cio.com.br/tecnologia/2017/01/23/fog-computing-e-o-novo-paradigma-para-a-internet-das-coisas-diz-cisco/>.

THE GUARDIAN. *I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets*, 2017. Disponivel em: <https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold>.

THE NEW YORK TIMES. *Sent to Prison by a Software Program's Secret Algorithms*, 2017. Disponivel em: <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html>.

UNCTAD. *Data protection regulations and international data flows:* Implications for trade and development, New York, 2016. Disponivel em: <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf>. Acesso em: 27 março 2018.

VIOLA, M. *Marco Civil da Internet.* Encontro sobre PLs de proteção de dados pessoais e direito ao esquecimento. Rio de Janeiro: [s.n.]. 2017.

WANG , Y.; KOSINSKI,. *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*. Journal of personality and social psychology , 2017.

WONG, J. C. *Mark Zuckerberg accused of abusing power after Facebook deletes 'napalm girl' post*. The Guardian, Setembro 2016. Disponivel em: <https://www.theguardian.com/technology/2016/sep/08/facebook-mark-zuckerberg-napalm-girl-photo-vietnam-war>. Acesso em: 27 março 2018.

WORLD SUMMIT ON THE INFORMATION SOCIETY. *Tunis Agenda for the Information Society*. [S.l.]. 2005.