UMA PERSPECTIVA DE DIREITOS HUMANOS PARA DECRIPTAR A ASCENSÃO DA INTERNET DAS COISAS (IOT)

Luca Belli

Professor de Governança e Regulação da Internet. FGV Direito Rio – Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas. *E-mail*: luca.belli@fgv.br.

Resumo: A Internet das Coisas (IoT, na sigla em inglês) é um fenômeno anunciado por seus proponentes como uma verdadeira propulsora da próxima revolução industrial, capaz de gerar ganhos consideráveis em termos de eficiência e crescimento. Porém, junto com as vantagens que a IoT pode determinar, parece necessário avaliar as consequências que tal fenômeno é susceptível de desencadear sobre o pleno gozo dos direitos humanos e fundamentais. O objetivo deste artigo é, portanto, investigar brevemente quais evoluções tecnológicas estão conduzindo a IoT – e sendo possibilitadas por ela –, e qual pode ser o impacto da IoT sobre os direitos dos indivíduos. O artigo analisa elementos que poderiam permitir aos poderes públicos e às empresas enfrentar os desafios da IoT favorecendo, de maneira sinérgica, o desenvolvimento de sistemas de IoT responsáveis, em conformidade aos Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos. Primeiramente, este artigo analisará o fenômeno da IoT, enfatizando a íntima ligação entre os fenômenos da IoT, *big data* e inteligência artificial. A segunda seção examinará brevemente o impacto que os fenômenos acima mencionados podem ter no pleno gozo dos direitos humanos e fundamentais, fornecendo alguns exemplos concretos. A seção final fornecerá algumas sugestões sobre como Estados e empresas podem implementar os princípios de forma eficaz.

Palavras-chave: Internet das Coisas. IoT. *Big data*. Inteligência artificial. Privacidade. Segurança. Princípios Orientadores da ONU sobre Empresas e Direitos Humanos.

1 Introdução: o fenômeno da Internet das Coisas (IoT)

A Internet das Coisas (IoT, na sigla em inglês) é um fenômeno anunciado por seus proponentes como uma verdadeira propulsora da próxima revolução industrial, capaz de gerar ganhos consideráveis em eficiência e crescimento "a uma taxa astronômica".[1] Porém, junto com as vantagens que sistemas de

[1] Ver Maddox (2018).

objetos interconectados podem determinar em termos de produtividade, parece necessário avaliar as consequências que sistemas de IoT são susceptíveis de desencadear sobre o pleno gozo dos direitos fundamentais.

Este artigo almeja, portanto, esclarecer alguns pontos essenciais do debate técnico e jurídico cujas interseções não podem ser desconsideradas ou subestimadas, a fim de compreender o impacto da evolução técnica sobre a eficácia e efetividade dos direitos humanos e fundamentais. Neste sentido, este artigo apresenta uma perspectiva de direitos humanos sobre a IoT e apela à construção de uma IoT responsável, baseada na implementação dos Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos (*UN Guiding Principles on Business and Human Rights* ou UNGPs,[2] na sigla em inglês), pelos Estados e empresas envolvidas em desenvolvimento, organização e implantação de sistemas de IoT.

A avaliação dos impactos da IoT sobre os direitos humanos e fundamentais encontra um primeiro obstáculo na definição mesma do conceito de IoT que é, por natureza, bastante flexível e, até o momento, não goza de uma acepção aceita universalmente.[3] No entanto, os diversos autores que realizam pesquisas sobre a IoT – e as distintas definições que cada um deles oferece – convergem destacando que a principal característica desse fenômeno é a conexão do mundo físico, composto por todas as "coisas", com o mundo digital. Já em 2010, refletindo sobre as diferentes dimensões da IoT, Atzori, Iera e Morabito (2010, p. 2787) argumentavam:

> A ideia básica desse conceito é a presença generalizada à nossa volta de uma variedade de coisas ou objetos – como tags de identificação por radiofrequência (RFID), sensores, atuadores, telefones celulares, etc. – que, por meio de esquemas de endereçamento exclusivos, são capazes para interagir uns com os outros e cooperar com outros objetos para alcançar objetivos comuns.

[2] Em julho de 2011, o Conselho de Direitos Humanos da Organização das Nações Unidas aprovou por consenso os UNPGs. Esses 31 Princípios são o resultado de seis anos de trabalhos liderados pelo Representante Especial do Secretário-Geral das Nações Unidas, Professor John Ruggie, e visam implementar os parâmetros "proteger, respeitar e reparar" apresentados por John Ruggie, em 2008. Os três pilares que fundamentam os UNGPs são: a obrigação dos Estados de proteger os direitos humanos; a responsabilidade das empresas de respeitar os direitos humanos; a necessidade de que existam recursos adequados e eficazes, em caso de descumprimento destes direitos pelas empresas. Veja-se Human Rights Council (2011).

[3] Para uma introdução à IoT veja-se Magrani (2018).

A União Internacional de Telecomunicações (UIT) destaca que a IoT deveria ser considerada uma "infraestrutura global para a sociedade da informação, possibilitando serviços avançados interconectando coisas (físicas e virtuais) com base nas tecnologias de informação e comunicação interoperáveis existentes e em evolução".[4] Conforme a definição da UIT, o Decreto nº 9.854, de 25.6.2019 define a IoT como "a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade".[5]

Todavia, apesar da ênfase da UIT e do governo brasileiro na "interoperabilidade" das coisas e redes que compõem a IoT, é importante destacar que o uso do termo "internet" pode ser enganoso, considerando que, com frequência, os sistemas de objetos conectados se caracterizam por serem redes fechadas, controladas para produtores de objetos, ao invés de redes de redes abertas e interoperáveis que caracterizam a internet.[6] Neste sentido, a maioria dos sistemas de objetos conectados poderia ser considerada "intranets" das coisas, ao invés de uma única rede de redes tal que a internet. Assim, apesar de utilizar o protocolo IP para comunicação de dados, as coisas não são obrigatoriamente conectadas a uma rede única, mas podem ser conectadas a redes fechadas cujo controle e gestão são centralizados nas mãos dos produtores de "coisas" – sejam tais coisas carros, câmaras, ou dispositivos que se podem vestir (os ditos *wearable devices*) como os relógios ou até sapatos conectados – ou dos provedores de infraestruturas de redes que permitem o funcionamento de tais coisas.

A IoT pode, portanto, ser definida como uma rede que conecta objetos físicos identificados de maneira exclusiva a redes eletrônicas e *software* que permitem a comunicação e o processamento de dados coletados por meio das "coisas". Os fabricantes de dispositivos e provedores de serviços geralmente exaltam a evolução de tal interconexão como facilitadora do surgimento de "tecnologias inteligentes", que tornam possíveis e facilitam fenômenos – caracterizados por um intenso *marketing* – como as "Cidades Inteligentes", "Agricultura Inteligente" e "Indústria 4.0", que são baseados na coleta e processamento generalizado de dados, possibilitados pela exploração de sistemas IoT.[7]

---

4 Ver ITU (2012).

5 O decreto institui o Plano Nacional de IoT, que pode ser considerado um dos pilares da Estratégia Brasileira de Transformação Digital (E-Digital), instituída pelo Decreto nº 9.319, de 21.3.2018, e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas, órgão colegiado cuja tarefa principal é supervisionar as ações no âmbito do Plano. A definição de IoT é fornecida pelo art. 2.I do Decreto nº 9.854, de 25.6.2019.

6 Ver Noura, Atiquzzaman e Gaedke (2018).

7 Ver BNDES (2017).

Na prática, a IoT já engloba bilhões[8] dos chamados dispositivos "inteligentes" que podem ser identificados de maneira exclusiva e são capazes de coletar, armazenar, processar e compartilhar uma ampla gama de dados sobre o funcionamento das próprias coisas e sobre ambiente – e, portanto, também sobre os indivíduos – em torno delas. De fato, o objetivo da IoT é facilitar a conexão de todos os objetos e dispositivos do dia a dia a redes eletrônicas, que podem compor a internet, mas também redes fechadas, como intranets privadas, para melhorar a coleta de dados e melhorar a eficiência por meio do processamento de dados.

A IoT se baseia no sucesso de vários facilitadores tecnológicos que possibilitam[9] a interconexão de bilhões de dispositivos. Devido ao seu potencial, o desenvolvimento da IoT é observado com grande atenção por vários atores, tanto do setor privado, particularmente operadoras de telecomunicações, provedores de serviços e fabricantes de dispositivos, quanto de órgãos públicos ávidos por moldar um ambiente regulatório de IoT capaz de facilitar negócios e atrair investimentos, enquanto previne, evita – ou pelo menos mitiga – os riscos de privacidade e segurança que os sistemas de IoT são susceptíveis de determinar.

Nesta perspectiva, a União Internacional de Telecomunicações argumenta que as capacidades de identificação, coleta de dados, processamento e comunicação da IoT devem fazer "uso total das coisas para oferecer serviços para todos os tipos de aplicações, garantindo que os requisitos de segurança e privacidade sejam cumpridos".[10] De fato, os dispositivos conectados e, consequentemente, os sistemas de IoT são instrumentais para implantar serviços baseados em capacidades de coleta e processamento de dados cada vez mais refinados, onipresentes e volumosos, capazes de aumentar eficiências em áreas como serviços de cidades inteligentes, segurança pública, saúde e sistemas de gerenciamento predial.

8 Ver IOT Analytics (2018).

9 Particularmente, a IoT depende da expansão de redes de internet móvel, da difusão e da redução de custos de tecnologias de sensores sem fio e nanotecnologias que podem ser incluídas em praticamente qualquer dispositivo fabricado junto com etiquetas de identificação por radiofrequência (RFID). RFID é um sistema de etiquetagem por meio de sinais de rádio que fornece dados de identificação para quaisquer mercadorias marcadas, a fim de torná-las facilmente rastreáveis, sem a necessidade de leitura de dados em códigos de barras para itens individuais. Conforme apontado pela UIT, "Dependendo da sua construção, as etiquetas RFID podem ter menos de um milímetro quadrado de área e serem mais finas do que uma folha de papel. Um dos aspectos mais cruciais dessas etiquetas eletrônicas é que elas permitem a identificação precisa de objetos e o encaminhamento dessas informações para um banco de dados armazenado na Internet ou em um servidor remoto. Dessa maneira, os recursos de processamento de dados e informações podem ser associados a qualquer tipo de objeto" (ITU, 2005).

10 Ver Rec. ITU-T Y.2060 (06/2012).

Como destacaremos na próxima seção, a ampla gama de dados coletados e compartilhados pelos dispositivos que fazem parte dos vários sistemas de IoT está de fato alimentando o processamento de dados complexos, produzindo conhecimentos que permitem aumentar a eficiência não somente dos processos pelos quais os dispositivos são utilizados, mas também dos dispositivos mesmos. Para entender as dimensões da IoT e seus desdobramentos é, portanto, essencial considerar a dimensão sistêmica da IoT. Como destaca Silvio Meira (2016, citado por MAGRANI, 2018, p. 70):

> a]s coisas não existem soltas, por aí. E não são, ou não deveriam ser, simplesmente, sensores e atuadores em rede. Isso seria diminuir muito o que se espera de #IoT, the internet of things, e reduzir seu potencial ao da velha e boa telemetria. Para que todo seu potencial possa ser capturado, as coisas têm que fazer parte de um sistema, de uma ou de um conjunto articulado de plataformas.

A IoT é, portanto, um conceito que compreende um crescente número de tecnologias capazes de expandir o alcance da internet no mundo físico, permitindo monitorar – de modo permanente e onipresente – o *status* dos objetos conectados e dos ambientes adjacentes. Nessa perspectiva, a interconexão de cada objeto também pode gerar riscos para a proteção da privacidade e dos dados pessoais dos indivíduos próximos às coisas conectadas, bem como para sua segurança pessoal e para a segurança pública, caso os dispositivos sejam hackeados. De fato, a possibilidade de controlar remotamente ou manipular dispositivos conectados pode levar a um efeito adverso no aproveitamento dos direitos fundamentais dos indivíduos, interferindo não apenas na privacidade dos indivíduos,[11] particularmente no que diz respeito à vida familiar, ao domicílio e à correspondência, mas também quanto à segurança pessoal, à não discriminação ou no acesso a informações.[12]

Quando tais redes e dispositivos não são concebidos, mantidos e protegidos da maneira mais responsável, seus usuários, bem como todas as pessoas que se encontram nos arredores de aparelhos conectados hackeados ou que podem ser monitoradas pelos transmissores embutidos nas coisas "inteligentes", podem sofrer consequências nefastas em um amplo espectro de direitos. Assim, a propagação de dispositivos "inteligentes" conectados no âmbito da IoT não determina simplesmente ganhos em eficiência, mas traz também novos desafios sociais, econômicos e jurídicos. Num contexto no qual bilhões de objetos inteligentes se

[11] Para uma ampla gama de exemplos de potenciais abusos dos direitos fundamentais causados pelos sistemas IoT, ver Privacy International ([s.d.]).

[12] Ver Leswing (2016).

inserem no nosso ambiente e nas nossas vidas cotidianas – frequentemente em ausência de nossa ciência ou consentimento –, parece ingênuo desconsiderar os impactos sobre privacidade e segurança gerados por essas evoluções tecnologias.

Nessa perspectiva, Estados e empresas envolvidas em sistemas de IoT devem atuar em sinergia, analisando riscos e elaborando e implementando políticas, regulações e adjudicações efetivas, levando a uma IoT plenamente compatível com o respeito dos direitos fundamentais das pessoas, em que a privacidade e a segurança das pessoas estejam no centro dos novos ecossistemas digitais. É importante analisar a IoT de modo meticuloso para entender as complexidades, os riscos e os benefícios desse fenômeno e estruturá-lo de maneira responsável.

O objetivo deste artigo é, portanto, investigar brevemente quais evoluções tecnológicas estão conduzindo – e sendo possibilitadas – pela IoT, qual pode ser o impacto da IoT sobre os direitos humanos e fundamentais dos indivíduos e quais elementos poderiam permitir que as partes interessadas, sejam de natureza pública ou privada, possam enfrentar os desafios da IoT. Particularmente, o artigo visa oferecer pistas para favorecer, de maneira sinérgica, o desenvolvimento de sistemas de IoT responsáveis, em conformidade aos UNGPs, considerando a relevância de tais princípios a fim não somente de especificar as obrigações dos atores públicos, mas também de orientar a atividade dos atores privados, norteando-a no pleno respeito dos direitos humanos. Nesta perspectiva, este trabalho será estruturado em três seções. A primeira seção deste artigo analisará o fenômeno da IoT, enfatizando a íntima ligação entre os fenômenos da IoT, *big data* e inteligência artificial. A segunda seção examinará brevemente o impacto que os fenômenos acima mencionados podem ter no pleno gozo dos direitos humanos e fundamentais, fornecendo alguns exemplos concretos. A seção final fornecerá algumas sugestões sobre como os Estados e as empresas de tecnologia que desenvolvem objetos conectados podem implementar os UNGPs de modo eficaz.

2 A interação entre IoT, *big data* e inteligência artificial

De acordo com Gartner (2014), a IoT alcançará 26 bilhões de unidades até 2020 – que é, por si só, um dado impressionante se comparado com menos de um bilhão de dispositivos conectados em 2009 – enquanto a Cisco (2016) prevê que 500 bilhões de dispositivos estejam conectados à internet até 2030. Tais estimativas permitem não somente imaginar o tamanho desse fenômeno mas compreender que a IoT não pode ser considerada uma perspectiva futura, e sim um fenômeno presente, no qual empresas estão investindo solidamente e o qual poderes públicos estão considerando para implementação de suas

próprias políticas. Portanto, é importante ressaltar que os sistemas de IoT serão onipresentes e estão penetrando no ambiente *off-line* em que existimos, sem nos deixar alternativas claras a fim de optar por não participar e evitar o impacto da conexão dos objetos conectados.

A integração entre os mundos físico e digital fomentada pela IoT e a capacidade de coleta de dados que ela facilita provavelmente afetará não apenas o desempenho dos serviços e dispositivos conectados, mas também poderá ter implicações diretas sobre os indivíduos. Notavelmente, o fato de objetos estarem permanentemente conectados a outros objetos, aplicações e redes de comunicação, e que tais objetos podem ser controlados remotamente, impacta diretamente os indivíduos. Esse impacto não se refere apenas à forma como os indivíduos interagem com os objetos, mas também, e crucialmente, às relações entre pessoas, entre pessoas e empresas, bem como entre pessoas, empresas e órgãos públicos.

De fato, devido ao inquestionável potencial de coleta, compartilhamento e processamento de dados, os sistemas IoT são considerados um elemento indispensável para alimentar serviços que se baseiam na exploração das análises de *big data*[13] e das capacidades da inteligência artificial[14] (IA), que estão impulsionando a evolução tecnológica do setor público e privado.[15] Neste sentido, o conceito de IoT pressupõe que qualquer tipo de objeto do nosso quotidiano possa ser conectado e conectável à internet, "de modo a dotá-los da inteligência necessária para interagir e, de algum modo, auxiliar a vida das pessoas por meio da coleta de dados físicos, processamento e promoção de respostas através de atuadores eletromecânicos".[16]

No entanto, parece importante enfatizar que, apesar do *hype* em torno da IoT dentro dos círculos da tecnologia, a maioria das pessoas sem uma capacitação técnica pode não saber que seus dados pessoais são coletados e compartilhados – de modo mais ou menos seguro – pelos objetos que podem ser encontrados nos ambientes em que vivem, trabalham ou brincam com os filhos.[17]

---

[13] O *big data* pode ser considerado "ativos de informação de alto volume, alta velocidade e alta variedade que exigem formas inovadoras e econômicas de processamento de informações para uma melhor percepção e tomada de decisão" Veja a entrada "Big Data" do glossário *Gartner IT* (http://www.gartner.com/it-glossary/big-data).

[14] O termo "inteligência artificial" tem fronteiras muito flexíveis e é muito amplo em escopo. Para Andrew Moore, decano de Ciência da Computação da Carnegie Mellon University, "A inteligência artificial é a ciência e a engenharia de fazer os computadores se comportarem de maneira que, até recentemente, pensávamos que era necessária inteligência humana". Ver High (2018).

[15] Ver *e.g.* GSMA (2015); Cisco (2016); IOT Analytics (2018).

[16] Ver Jesus Junior e Moreno (2015).

[17] Um exemplo notável é o caso da CloudPets, uma série de ursos de pelúcia conectados produzidos pela Spiral Toys, que utiliza reconhecimento de voz e um aplicativo que se conecta via Bluetooth, que pode ser

Nesse contexto, na ausência de um esforço conjunto público-privado de conscientização dos usuários e promoção de transparência em relação aos impactos da IoT, a implantação de tais sistemas promete gerar confusão e até enganar os indivíduos, que podem nem perceber as minúsculas etiquetas RFID e sensores que estão embutidos nos dispositivos conectados, tornando quase impossível entender que objetos do dia a dia estão conectados à internet e são programados para coletar, transmitir e processar dados sobre seu ambiente ao redor.

Essa ambiguidade deve, portanto, ser corrigida pelo desenvolvimento de políticas e marcos regulatórios claros e eficazes, capazes de ajudar os desenvolvedores de IoT a exercerem sua responsabilidade social corporativa, ao mesmo tempo em que despertam o desconhecimento dos indivíduos sobre o impacto que os sistemas IoT causarão em seu ambiente e fornecem indicações sobre como obter um remédio jurídico aos eventuais efeitos abusivos do uso de IoT. Particularmente, estruturas robustas de proteção de dados e cibersegurança são especialmente relevantes para promover o desenvolvimento sustentável dos sistemas de IoT, evitando que os indivíduos sejam enganados e que os dados pessoais sejam utilizados de maneira abusiva. Neste sentido, o BNDES, em seu Relatório do Plano de Ação de IoT de 2017, destaca:

> Para além dos desafios na regulamentação de telecomunicações, é essencial endereçar os atuais gargalos nos temas de privacidade e proteção de dados pessoais e de segurança da informação. Embora se trate de temas maiores do que IoT, eles são catalisadores para o seu desenvolvimento adequado, em especial em ambientes como o de cidades e de saúde.[18]

Essa consideração torna-se ainda mais significativa considerando o íntimo entrelaçamento existente entre a IoT e dois fenômenos relacionados, *big data* e IA, que a IoT pode nutrir com um fluxo contínuo de dados pessoais e não pessoais muito diversos. Como destaca o Information Commissioner's Office britânico, os termos *big data* e IA são frequentemente usados de modo intercambiável, mas há diferenças sutis entre os conceitos. Por um lado, os *big data* analisam conjuntos maciços de dados muito heterógenos, em tempo real para criar modelos preditivos sobre algum aspecto do mundo. Assim as inferências desses

facilmente hackeado, com consequências potencialmente nefastas para a privacidade das crianças e dos pais que interagiam com os brinquedos. Tais consequências foram expostas, em 2017, quando hackers acessaram o banco de dados da CloudPets, sequestrando informações sobre mais de 800.000 pessoas, incluindo endereços de *e-mail*, senhas e gravações de voz de crianças. Ver NG (2018).

[18] Ver BNDES (2017, p. 19).

modelos são usadas para prever e antecipar possíveis eventos futuros. Por outro lado, os programas de IA não analisam "linearmente" os dados, ou seja, não precisam considerar os conjuntos de dados da maneira como foram originalmente programados. Em vez disso, eles aprendem com os dados para responder de modo inteligente aos desafios determinados para novos dados e adaptar suas respostas adequadamente, conferindo aos computadores comportamentos que seriam considerados "inteligentes" nos seres humanos.[19]

Neste contexto, os sensores embutidos nos objetos conectados representam uma fonte de dados extremamente relevante e valiosa, em termos não somente quantitativos, mas também qualitativos. Os dados coletados no âmbito da IoT podem ser utilizados para melhorar a modelagem preditiva oferecida pelos *big data*, mas também para treinar aplicativos de IA. Por exemplo, dados de transportes públicos, que podem ser pessoais, como dados gerados para cartões com etiquetas RFID de passageiros, e não pessoais, como geolocalizações GPS de ônibus ou dados de semáforos, podem alimentar análises de *big data* voltadas a definir modelos preditivos do trânsito cidadão e, consequentemente, melhorar a viabilidade.

Por outro lado, dados coletados por sensores de IoT podem também ser utilizados para permitir aos computadores aprender e elaborar respostas automaticamente. O caso dos veículos autônomos parece particularmente explicativo. Carros conectados são "coisas" capazes de gerar quantidades de dados impressionantes a fim de alimentar inteligência artificial de tipo automotivo. Os carros autônomos da Tesla podem ser considerados um exemplo notável de "intranet das coisas", baseada na interconexão no âmbito de uma rede fechada de automóveis que produzem e trocam dados para poder aprimorar continuamente as funções dos veículos. Tal aprimoramento contínuo é possível graças ou *machine learning*, ou aprendizagem por máquina, alimentado pelo processamento de dados coletados por milhares de sensores que se encontram em cada veículo Tesla. Como destaca o CEO da empresa, Elon Musk: "Toda a frota da Tesla opera como uma rede. Quando um carro aprende algo, todos aprendem".[20]

As soluções de IoT já estão implementadas em vários setores, não somente no que diz respeito aos carros conectados, mas também em serviços de saúde a distância, medição inteligente para serviços públicos como gás ou eletricidade. Em todos esses setores as análises de *big data* e IA baseadas nos dados coletados por milhares ou milhões de sensores conectados estão sendo implementadas por vários[21] atores empresariais. Por um lado, as análises de *big data* e os

[19] Ver ICO (2017, p. 7).
[20] Ver a entrevista de Elon Musk, em Fehrenbacher (2015).
[21] Ver Cisco (2016); IOT Analytics (2018).

aplicativos de IA são o(s) "facilitador[es] essencial[is] para a realização do pleno potencial da IoT",[22] pois contam com o processamento de conjuntos de dados massivos, reunindo dados de diferentes origens – incluindo, por exemplo, dados de localização de dispositivos específicos via GPS, publicações em redes sociais, metadados de comunicações etc. – que são examinados algoritmicamente para encontrar correlações. Por outro lado, os recursos de coleta de dados fornecidos pelos sistemas de IoT tornam-se instrumentais para explorar plenamente o potencial do *big data* e da IA, que são baseados no uso extensivo de grandes volumes de dados para melhorar a tomada de decisões ou a eficiência de produtos e serviços.

Para entender a correlação entre o fenômeno da IoT e *big data*, bem como as implicações desses fenômenos, parece útil oferecer dois exemplos de como os dados coletados e gerados por uma multiplicidade de coisas conectadas podem ser combinados para alimentar *big data* e IA para serviços públicos e privados. Um exemplo clássico é o estabelecimento dos chamados serviços de cidades inteligentes, em que dados oriundos de fontes como sensores instalados em transportes públicos e veículos policiais, luzes conectadas (semáforos) e informações sobre eventos públicos podem ser combinados para prever e otimizar o fluxo de tráfego em tempo real e identificar as áreas que necessitam de atenção urgente das forças de ordem. O setor de mídia e entretenimento também é um exemplo de como os dados de IoT podem enriquecer as análises de *big data* e de IA, cruzando as informações coletadas e geradas por plataformas digitais, como serviços de *streaming* de música ou vídeo e dispositivos conectados, com os dados coletados por TVs ou alto-falantes conectados, tais que o período de tempo e os momentos no dia nos quais um indivíduo utiliza uma TV inteligente ou os programas assistidos ou ainda os endereços IP do usuário.

Neste sentido, uma pesquisa conjunta da Northeastern University e o Imperial College London examinou as atividades de compartilhamento de dados de 81 diferentes dispositivos "inteligentes" comumente encontrados nas casas das pessoas – tais que TVs inteligentes, alto-falantes de áudio inteligentes e campainhas conectadas – e revelou que 72 dos 81 dispositivos de IoT coletavam dados pessoais de maneira desproporcionada compartilhavam dados com terceiros completamente não relacionados ao fabricante original.[23] Essa análise parece particularmente relevante por ter destacado que os dados coletados e compartilhados para a maioria dos dispositivos vai muito além das informações básicas sobre o dispositivo físico sendo usado, incluindo um amplo espectro de

[22] Ver GSMA (2015).
[23] Ver Ren *et al.* (2019).

informações de caráter pessoal como endereços IP e dados de localização, junto com especificações e configurações do dispositivo, hábitos de uso etc. De fato, essa coleta e processamento de informações permitirá obter um entendimento mais profundo, inferir padrões e tomar decisões baseadas em dados que estão se tornando extremamente valiosos para prever os interesses do público, extrair *insights* sobre grupos específicos de clientes e enviar anúncios personalizados que possam direcionar os comportamentos individuais da maneira mais eficiente possível.[24]

No entanto, cabe destacar que a coleta de grandes quantidades de dados, de um amplo espectro de fontes e sensores, pode ocorrer no desconhecimento dos indivíduos sobre quais dados são coletados, por plataformas e aplicativos, e por "coisas" conectadas. Além disso, é importante ressaltar que os principais critérios que impulsionam o *design* e a implementação das análises de *big data* e das capacidades de IA, bem como o *design* dos sistemas de IoT, podem não ser o respeito aos direitos fundamentais dos indivíduos, mas sim a minimização de custos e a maximização do lucro privado. Considerando que, para maximizar eficiência, controle e lucros, os atores privados, bem como os públicos, podem ser tentados a coletar o maior número possível de dados para alimentar análises de *big data* e aplicativos de IA. Cabe destacar que a falta de regulação apropriada pode transformar tais tecnologias, impulsionadas pela IoT, em uma ferramenta para vigilância massiva,[25] tomando decisões algoritmicamente em uma perspectiva de eficiência que, todavia, é susceptível de discriminar indivíduos ou populações específicas.[26]

Uma literatura crescente já demonstrou que a automatização da tomada de decisões pode levar à exclusão de grupos inteiros do acesso a direitos, serviços ou oportunidades específicas, com base em modelos preditivos – potencialmente enviesados – elaborados por algoritmos opacos.[27] É importante ressaltar que os enormes conjuntos de dados que os sistemas de IoT prometem gerar e as capacidades sensoriais onipresentes que caracterizam os sistemas de IoT podem não apenas maximizar a inteligência preditiva, mas também capacidades de

[24] Neste sentido ver Zuboff (2019).

[25] Neste sentido, veja as análises desenvolvidas por Howard (2015) e Weber (2015).

[26] Um exemplo revelador foi fornecido pela análise da organização sem fins lucrativos ProPublica sobre o funcionamento de uma ferramenta algorítmica utilizada para calcular a pontuação criminal de indivíduos, empregada por vários escritórios do Ministério Público nos EUA para prever quem iria reincidir. A análise identificou disparidades raciais significativas, demonstrando que o sistema "era particularmente suscetível a sinalizar falsamente os réus negros como futuros criminosos, erroneamente rotulando-os deste modo a quase o dobro da taxa dos réus brancos. Os réus brancos foram erroneamente rotulados como de baixo risco com mais frequência do que os réus negros". Ver Angwin *et al*. (2016).

[27] Ver O'Neil (2016) e Pasquale (2015).

vigilância facilitadas pelas tecnologias de IA, levantando importantes questões de segurança e privacidade, enquanto preveem e automatizam um número crescente de aspectos das nossas vidas diárias. Em sua essência, a IA analisa e otimiza os dados para uma variedade de propósitos, abrangendo desde assistência por voz até a previsão de hábitos de consumo, carros autônomos ou diagnósticos médicos. Portanto, a combinação de dados gerados pela IoT e IA pode ser utilizada para ajudar os indivíduos em suas tarefas diárias, aumentando a produtividade e melhorando os cuidados de saúde, mas também poderia dar origem a mais cenários distópicos, baseados na vigilância onipresente e em decisões definidas pela IA que são diretamente implementadas no mundo *off-line*, cada vez mais composto de infraestruturas conectadas e de prédios e dispositivos inteligentes.

A interconexão de todos os objetos (a serem) produzidos e os sistemas de IA ou o uso de sistemas de IoT para alimentar as análises de *big data* estão, portanto, prestes a afetar potencialmente todos os aspectos de nossas vidas e todos os ambientes nos quais vivemos. Tal cenário tem implicações notáveis para os direitos dos indivíduos. As seções a seguir identificarão alguns dos desafios mais substanciais, que tanto a Administração Pública quanto os empresários precisam abordar com a maior urgência possível, a fim de garantir que o desenvolvimento da IoT e sua interação com *big data* e IA sejam um fator positivo de mudança em vez de propulsores de um futuro distópico.

3 Perfis de direitos humanos levantados por sistemas de IoT

O surgimento de sistemas de IoT e a possibilidade de que tais sistemas coletem e forneçam continuamente dados para tomar decisões sobre seres humanos levantam várias questões de políticas públicas relacionadas à governança de IoT,[28] com particular atenção à privacidade, segurança, livre desenvolvimento da personalidade e não discriminação.

Os dados coletados e gerados por sensores embutidos em objetos do cotidiano, como *smartphones*, brinquedos, dispositivos *wearables* e mobiliário urbano podem ser precisos o suficiente para entender e prever o estilo de vida, comportamento de consumo e outros padrões relevantes de grupos inteiros de indivíduos ou de uma pessoa em específico. Como apontado na seção anterior, a disseminação de dispositivos conectados e a incorporação de sensores em todas as "coisas" de nosso uso quotidiano transformarão a coleta de dados em uma

[28] Ver *e.g.* European Commission (2013) e Weber (2015).

prática permanente e onipresente, dando origem a várias condutas e modelos de negócios que têm o potencial para infringir um amplo espectro de direitos humanos.

De fato, a variedade de riscos aos quais os indivíduos estão expostos[29] em ambientes de IoT não se limita à perda de privacidade e segurança, possibilitada pelos dispositivos conectados que coletam dados permanentemente e, posteriormente, armazenam, processam e os transferem de modo inseguro. Pelo contrário, tais riscos são amplificados consideravelmente, por um lado, pela exploração de sistemas de IoT para alimentar *big data* e IA capazes de tomar decisões sobre indivíduos e, por outro lado, pela possibilidade de tal conexão entre computação e dispositivos poder moldar concretamente o ambiente físico em que os indivíduos vivem e determinar verdadeiros impactos e consequências físicas nos indivíduos em contato com as demais coisas conectadas. Um exemplo particularmente evidente, neste sentido, é o crescente uso de câmeras conectadas no âmbito das ditas "Cidades Inteligentes" a fim de automatizar serviços de segurança pública. Como recentemente comprovado para uma pesquisa do Carnegie Endowment for International Peace, pelo menos setenta e cinco países globalmente usam ativamente as tecnologias de IA para fins de vigilância, desenvolvendo sistemas de reconhecimento facial no âmbito de plataformas de cidades inteligentes.[30]

Todavia, cabe destacar que o nível de "inteligência" dessas iniciativas deve ser considerado com cuidado. Por um lado, as decisões tomadas por meio de reconhecimento facial não são infalíveis e podem determinar um número elevado de falsos positivos ou negativos, especialmente quando o reconhecimento visa populações não caucásicas.[31] Por outro lado, quando sistemas de IoT alavancam a tomada de decisão algorítmica, os algoritmos podem ser incapazes de fornecer uma explicação no que diz respeito ao raciocínio que determinou a decisão.

Este é frequentemente o caso de modelos de *machine learning* ditos de aprendizado não supervisionado, um tipo de aprendizado por máquina que não envolve a criação algorítmica humana, mas, ao contrário, se baseia integralmente no processamento de dados por algoritmos desenvolvido autonomamente pela IA. Quando organizações utilizam esse tipo de IA para processar dados coletados por meio de câmaras, sensores ou outros objetos conectados, é, portanto, possível que decisões sejam tomadas sem poder comunicar para o destinatário da decisão

[29] Para uma seleção ilustrativa dos riscos à privacidade aos quais os indivíduos são expostos quando em contato com os sistemas de IoT, ver Privacy International ([s.d.]).

[30] Ver Feldstein (2019).

[31] Neste sentido, ver Garvie, Bedoya e Frankle (2016) e Noble (2018).

qual foi o raciocínio que determinou a decisão nem quais dados fundamentam tal raciocínio.[32]

Cabe ressaltar que a perda de controle individual sobre dados pessoais torna-se um cenário muito provável, considerando não apenas os recursos de coleta de dados permanentes e automáticos de objetos conectados, mas também que dados coletados por dispositivos e sensores conectados são frequentemente "reaproveitados" para serem processados para diferentes finalidades. Tais objetivos podem ser substancialmente diferentes do mero funcionamento das "coisas" conectadas e o processamento pode ser executado por uma entidade diferente daquela originalmente responsável pela coleta de dados, por exemplo no caso em que os dados coletados pela empresa vendedora de um relógio ou uma geladeira conectada sejam compartilhados ou cruzados por outras empresas responsáveis para as análises de *big data* ou AI e, potencialmente, compartilhada com um número não definido de terceiros.

Além disso, o fato de os dispositivos conectados poderem coletar dados automaticamente, em vez de solicitar que os indivíduos forneçam tais dados voluntariamente, apresenta sérios riscos em relação à conscientização individual e ao consentimento para a coleta de dados. É o caso, por exemplo, de sensores em áreas públicas ou em transportes públicos – cada vez mais comuns em projetos de cidades inteligentes –[33] que capturam uma ampla gama de dados pessoais, como imagens de transeuntes ou identificadores exclusivos de telefones celulares das pessoas.[34] É improvável que esse tipo de coleta e processamento esteja em conformidade com os princípios básicos de proteção de dados, como legalidade, justiça e transparência,[35] que estão na base de estruturas de privacidade em mais de 120 países em todo o mundo.[36]

Ao contrário, para respeitar a privacidade de dados dos indivíduos, as entidades que implantam e implementam sistemas IoT devem garantir que suas

[32] Ver Schider (2018, p. 137).

[33] Veja *e.g.* o exemplo de lixeiras conectadas em Londres, que coletavam ilegalmente identificadores de celular, e as portas conectadas das estações de metrô de São Paulo que coletavam ilegalmente imagens de passageiros, relatadas por Miller (2013) e Amigo (2018).

[34] Neste sentido, a Privacy International relatou a compra de coletores de IMSI por várias forças policiais britânicas. IMSI é o acrônimo, em inglês, para "Identidade Internacional de Usuário Móvel", um número exclusivo para cada cartão SIM, e um receptor IMSI é uma "tecnologia altamente intrusiva que localiza e rastreia todos os telefones móveis que estão ligados e conectados a uma rede em uma determinada área. Ele faz isso fingindo ser uma torre de telefone celular, enganando o telefone para se conectar a ele e revelando seus dados pessoais sem o seu conhecimento. Alguns coletores de IMSI podem até mesmo ser usados para monitorar suas chamadas e editar suas mensagens sem o seu conhecimento. […] Assim que seu telefone é levado a se conectar a um receptor IMSI, ele revela esse número". Ver Privacy International (2019).

[35] Veja Greenleaf (2018).

[36] Veja Greenleaf (2018).

práticas de coleta de dados sejam compatíveis com a legislação e, principalmente, que os indivíduos cujos dados são coletados sejam devidamente informados sobre que tipo de dados sobre eles são coletados e com qual finalidade, e que mantenham a possibilidade de exercer a escolha livre de não serem sujeitos de tal coleta. Todavia, parece ambicioso vislumbrar que, em um ambiente cada vez mais povoado por sensores e objeto conectados, o indivíduo possa ser informado devidamente de como serão utilizados os dados coletados por cada sensor e, por consequência, exprimir seu consentimento informado. O consentimento, apesar de ser uma pedra angular da maioria dos marcos regulatórios sobre privacidade, já foi objeto de abundantes críticas por causa de sua ineficiência como instrumento de proteção de dados pessoais.[37] O aumento exponencial de pontos de coleta de dados promovido pela IoT é um cenário que de fato frustra adicionalmente o uso do consentimento como base jurídica apropriada para justificar a coleta e processamento de dados.

Esse cenário é particularmente flagrante quando os dados coletados por meio de sistemas de IoT alimentam as análises de *big data*. Embora possa ser argumentado que os propósitos das análises de *big data* são frequentemente desconhecidos antes da análise e que o interesse de tais análises é precisamente a capacidade de revelar inferências e correlações inesperadas, é importante enfatizar que isso não pode ser uma justificativa para operar análises opacas e enganar os titulares de dados ou induzi-los ao erro. Dessa forma, quando os dados pessoais são coletados por meio de dispositivos conectados e utilizados para alimentar grandes conjuntos de dados, é essencial que os indivíduos estejam cientes de que a coleta de dados está em andamento e que o objetivo secundário da análise é compatível com o original. Como exemplo, os dados coletados por meio do mobiliário urbano conectado para analisar e aumentar a segurança urbana não devem ser usados para traçar o perfil dos transeuntes para fins comerciais, como exemplo, para determinar o valor de seus prêmios de seguro (vida, saúde ou carro).

Nesta perspectiva, é útil enfatizar que uma distinção deve ser feita entre a coleta de dados via sistemas de IoT para potencializar análises cujo propósito é a detecção de tendências gerais e a coleta e processamento de dados que são operados para extrair inferências sobre indivíduos e tomar decisões que os afetam. Neste último caso, a combinação de sistemas de IoT e análise de *big data* pode não apenas ser incompatível com os propósitos originais para os quais os dados foram coletados pelos dispositivos e sensores conectados, mas também criar novos dados pessoais sobre os indivíduos.

[37] Veja Calo (2013); Solove (2013) e Belli, Schwartz e Louzada (2017).

Um exemplo revelador poderia ser a utilização de sensores automotivos para coletar e processar grandes quantidades de dados sobre determinado veículo, por exemplo, para fins de manutenção e aprimoramento do desempenho do carro, mas também para identificar padrões no comportamento do motorista e criar um perfil para determinar o valor do prêmio do seguro. Nessa perspectiva, as companhias que utilizam dados coletados pelos sistemas de IoT devem ser capazes de encontrar o momento adequado em que as informações apropriadas podem ser fornecidas aos indivíduos afetados sobre quais dados são coletados e com que finalidade, para que eles possam manter uma escolha significativa para autorizar ou negar a coleta e (tipos específicos de) processamento de seus dados.

Além disso, é importante sempre ter em mente a natureza sistêmica da IoT para perceber a interdependência das questões de privacidade e segurança. A conexão de milhares ou milhões de dispositivos diversos traz um número proporcional de vulnerabilidades e, portanto, riscos que podem ser explorados por ciber-atacantes cujo nível de sofisticação é cada vez maior. Assim, práticas como encriptação de dados, desidentificação de dados pessoais e implementação de mecanismos rígidos de controle de acesso são essenciais para evitar a disseminação indesejada de dados e proteger efetivamente a privacidade de todas as pessoas afetadas por um sistema IoT específico.

Com relação ao impacto que os sistemas de IoT podem ter na segurança, é importante ressaltar a dupla dimensão de tal questão política, englobando tanto o direito dos indivíduos à segurança quanto a segurança das informações. Conforme demonstrado por Miller e Valasek (2015), que elaboraram um método para controlar remotamente os freios e o acelerador de carros Jeep conectados, a invasão de sistemas IoT desprotegidos pode ter consequências diretas na incolumidade e até na vida dos indivíduos. Por outro lado, as preocupações de cibersegurança podem afetar diretamente a segurança pública, pois sistemas IoT comprometidos podem permitir que *hackers* acessem e controlem remotamente infraestruturas públicas, como máquinas conectadas em hospitais, semáforos, usinas elétricas etc.

Nessa perspectiva, a segurança da IoT não é apenas essencial para preservar a privacidade ou a segurança dos indivíduos, mas também para garantir a segurança pública contra infiltrações e manipulações indesejadas. Portanto, a segurança de todos os componentes dos sistemas de IoT deve ser considerada uma prioridade indissociável das proteções de privacidade, em vez de uma preocupação secundária ou opcional para os desenvolvedores.

Por fim, deve-se enfatizar a crescente interdependência entre os sistemas de IoT e os recursos de *software* e computação fornecidos pelas empresas de IA. A influência dessas empresas em desenvolvedores de dispositivos conectados pode ser explicada quando consideramos a importância fundamental do *software*

e da capacidade computacional para garantir que os dispositivos conectados funcionem sem problemas. A Bloomberg Technology relatou recentemente um exemplo de tal influência, destacando que a Alphabet (empresa-mãe do Google) e a Amazon, que fornecem os principais programa de *software* de assistência de voz, os quais são utilizados por uma ampla variedade de dispositivos domésticos conectados, estão solicitando ativamente aos fabricantes de dispositivos que modifiquem os parâmetros dos dispositivos para que estes recebam fluxos contínuos de dados que possam ser coletados e processados pelos fornecedores de *software*. Nesse cenário, os usuários de dispositivos inteligentes podem estar inconscientemente –[38] e provavelmente involuntariamente – fornecendo uma ampla gama de informações sobre o uso do dispositivo inteligente, independentemente de o dispositivo estar ligado ou desligado.[39]

Consciente do fato de que objetos e sensores conectados permitem a coleta e o compartilhamento constante de dados, torna-se essencial que o indivíduo mantenha o conhecimento e controle sobre quando e como seus dados pessoais são coletados, por quem e com que fins. Além disso, para facilitar o uso seguro de dispositivos conectados, torna-se essencial utilizar mecanismos confiáveis para autenticação e autorização, capazes de impedir o acesso não autorizado a sistemas IoT e preservar a integridade dos dados.[40] Por fim, o uso de técnicas de anonimização de dados torna-se cada vez mais importante para facilitar o uso e a reutilização de dados coletados por meio de sistemas de IoT, reduzindo os riscos relacionados à perda de controle sobre os dados pessoais.

4 Conclusões: rumo a sistemas responsáveis de IoT

Para maximizar os benefícios e reduzir – e idealmente eliminar – os riscos determinados pelo surgimento dos sistemas de IoT, as partes interessadas, que

[38] A situação de desconhecimento geral sobre o alcance das capacidades de coleta de dados da IoT é exemplificada pelo recente anúncio do Google de que seu sistema de segurança e alarme Nest Secure seria atualizado, permitindo que os usuários aproveitem a tecnologia de assistente virtual do Google, para surpresa de todos usuários do Nest que não sabiam nem poderiam saber que o Nest Secure possuía um microfone. De fato, antes do anúncio de atualização, a existência de um microfone dentro dos componentes do Nest Secure nunca foi divulgada. Ver Bastone (2019).

[39] Assim, "as televisões devem informar o canal que está sendo assistido e as fechaduras inteligentes devem manter a empresa informada se o ferrolho da porta da frente está ou não engatado. Essa informação pode parecer banal se comparada ao software de geolocalização de smartphones que acompanha você por aí, mas até mesmo dispositivos simples, como lâmpadas, podem permitir às empresas de tecnologia extrair informações sobre seus clientes e usar os dados para fins de marketing". Ver Day (2019).

[40] Para uma revisão sobre mecanismos de autenticação, confidencialidade e controle de acesso, ver Sicari *et al*. (2015, p. 147-151).

sejam entidades públicas ou privadas, são chamadas a cooperar, tomando como inspiração dos UNGPs, para definir modelos de governança responsável de IoT, no âmbito dos quais os Estados e as empresas devem implementar o dever do Estado de proteger os direitos humanos, a responsabilidade corporativa de respeitar os direitos humanos e, juntamente, garantir acesso para remediar vítimas de abusos relacionados a negócios. Neste sentido, os Estados devem assumir seu dever de proteger os indivíduos contra abusos de direitos humanos desenvolvendo estratégias, políticas, regulamentos e mecanismos de adjudicação adequados que garantam a proteção da privacidade e segurança e definam claramente limites para que a IoT não seja usada para causar danos a indivíduos.

As empresas devem cumprir sua responsabilidade de respeitar os direitos humanos, agindo com a devida diligência, avaliando quando os sistemas de IoT podem ter impactos adversos sobre os indivíduos e projetar produtos e serviços que priorizem o respeito aos direitos dos indivíduos. Além disso, tanto os atores públicos como privados devem fornecer acesso a recursos efetivos, tanto judiciais quanto extrajudiciais, para as vítimas de qualquer dano produzido pelo uso de sistemas IoT.

Os governos e os atores comerciais devem desenvolver e implementar conjuntamente planos de IoT, começando pelo desenvolvimento de estruturas para avaliação de riscos da segurança de IoT, categorizando dispositivos de IoT de acordo com riscos e vulnerabilidades e, mais importante, avaliando o nível de disseminação de um produto conectado no mercado. Em segundo lugar, os atores públicos e privados devem promover – e os indivíduos devem exigir – a adoção de boas práticas para o desenvolvimento de *software* em todos os dispositivos de IoT. Essas práticas incluem privacidade e segurança desde a concepção[41] e durante todo o ciclo de vida de desenvolvimento de cada elemento que compõe o sistema IoT, bem como a possibilidade de atualizar e corrigir o *software*, gerenciar a identidade do usuário, e cuidar do estabelecimento de um ponto de contato permanente para sinalizar a existência de vulnerabilidades de *software* e *hardware*.

É importante ressaltar que um elemento essencial de qualquer estratégia que vise implementar com sucesso os UNGPs é buscar o envolvimento da sociedade civil. A esse respeito, os usuários de dispositivos conectados e o público em geral devem ter um papel fundamental na governança da IoT. A comunicação e a educação do público são elementos-chave e não devem ser vistos como processos unilaterais, mas como formas de informar e contribuir mutuamente para

[41] Isso significa que as considerações de privacidade e segurança devem ser incorporadas em todas as etapas do processo, desde a concepção, começando pela realização de avaliações de impacto de privacidade por meio do *design*, desenvolvimento e garantia de qualidade do sistema IoT.

sistemas de IoT mais seguros e confiáveis. O compartilhamento de informações sobre vulnerabilidades de *software* e dispositivos é um nítido exemplo de como a cooperação de múltiplos atores interessados não é somente útil, mas necessária. De fato, a implementação de sistemas IoT seguros requer um esforço colaborativo, já que apenas os interessados podem identificar e corrigir vulnerabilidades para proteger todo o sistema. Por outro lado, as políticas nacionais – inclusive em relação à educação – são essenciais para aumentar a conscientização sobre os desafios da IoT. As estruturas legais devem considerar o conhecimento individual e o consentimento como requisitos essenciais para a coleta de dados pessoais, pois cada pessoa deve poder escolher se quer fazer parte de um sistema IoT ou não, e a coleta e o processamento de dados nunca devem ser impostos arbitrariamente.

A transparência deve ser garantida para que as pessoas sejam adequadamente informadas sobre a natureza e a finalidade da coleta de dados e tenham informações claras e inteligíveis sobre quais dados pessoais são coletados, com quem essas informações são compartilhadas, bem como como acessar e retificar ou excluir esses dados a qualquer momento. Para esta última medida, o desenvolvimento de marcos regulatórios nacionais que garantam um nível de proteção de dados significativo, em um ambiente em que a IoT, IA e *big data* são práticas comuns, deve ser visto como um elemento essencial.

Os Estados devem, no mínimo, dispor de uma estrutura adequada de proteção de dados, desenvolvendo as seguintes ações:

1. obter consentimento para a coleta de dados, fornecendo informações significativas;
2. minimizar a quantidade de dados coletados para evitar possíveis riscos e abusos;
3. garantir que os titulares dos dados tenham a possibilidade de facilmente acessar dados pessoais;
4. garantir que os titulares dos dados tenham a possibilidade de facilmente retificar e excluir dados pessoais;
5. adotar todas as disposições necessárias para manter seguros os dados pessoais.

Por outro lado, para cumprir com sua responsabilidade de respeitar os direitos humanos, os atores do setor privado devem, no mínimo:

1. adotar um compromisso de respeito aos direitos humanos nos termos de uso dos produtos e serviços fornecidos;
2. realizar um processo de devida diligência em direitos humanos para identificar, prevenir, mitigar potenciais consequências negativas de seus produtos e serviços sobre os indivíduos e explicar como se responsabilizam

para seus impactos e planejam evitar consequências negativas sobre direitos humanos; e

3. dispor de processos efetivos para permitir a remediação de quaisquer impactos adversos aos direitos humanos que eles causam ou para os quais contribuam.[42]

Além disso, maneiras inovadoras de permitir que indivíduos expressem seu consentimento para (certos) tipos de processamento de dados pessoais também devem ser exploradas, mudando o foco da proteção de dados para uma abordagem de *design thinking*, em vez de depender de uma abordagem estritamente jurídica baseada na clássica estratégia de notificação e consentimento, que mostrou ter limites claros.[43] A esse respeito, o conceito de "Controle de Dados desde a Concepção"[44] (DCD, na sigla em inglês) deve ser explorado pelos formuladores de políticas para complementar a abordagem clássica de privacidade desde a concepção por meio da implementação de ferramentas tecnológicas apropriadas colocando os indivíduos no centro do processamento de dados, permitindo que eles escolham quais dados pessoais sobre eles podem ser processados e para quais fins.

O conceito DCD visa expandir a privacidade desde a concepção, promovendo a adoção de ferramentas de controle de dados interoperáveis, permitindo que os indivíduos definam como seus dados podem ser utilizados e que tais opções sejam "legíveis por máquina"[45] no momento da coleta de dados pessoais.[46] O uso dessa abordagem, implementada por meio de soluções tecnológicas tais que o protocolo User-Managed Access (UMA), desenvolvido pela iniciativa Kantara,[47] colocaria os indivíduos no centro, permitindo que os dispositivos e *softwares* dos sistemas de IoT que coletam e processam dados entendam e respeitem automaticamente as opções dos usuários em relação aos dados. Além disso, o conceito de DCD pode ser adequado para enquadrar sistemas IoT, já que indivíduos poderiam predefinir, por meio de soluções interoperáveis, como eles querem que seus dados sejam

[42] Ver Belli, De Filippi e Zingales (2015).

[43] O fato de serem apresentados aos indivíduos avisos de privacidade complexos e legalistas aos quais podem consentir, para usufruir de determinado serviço, ou recusar, perdendo assim a opção de usar o serviço desejado, mostra os limites da abordagem de notificação e consentimento em relação à liberdade individual. Esse cenário binário de tudo ou nada demonstra que o atual modelo de consentimento é ilusório, transformando uma ferramenta que supostamente deveria capacitar indivíduos a fazer escolhas informadas em uma ferramenta para confundir os usuários por meio de termos contratuais que não serão lidos, e transformando o consentimento à exploração de seus dados pessoais no verdadeiro preço dos serviços *on-line*.

[44] Ver Belli, Schwartz e Louzada (2017).

[45] Essa expressão designa um formato que pode ser facilmente processado por um computador.

[46] Id.

[47] Veja-se Machulak *et al*. (2010).

coletados e processados, em vez de terem que expressar seu consentimento ou não à coleta de dados operada para cada objeto conectado.

Tal dicotomia, geralmente proposta por estruturas de proteção de dados e baseada em aceitar a perda de controle sobre os dados em troca da possibilidade de utilizar os serviços, ou negar o acesso aos dados, perdendo a possibilidade de utilizar os serviços, é de fato altamente ineficiente, pois não permite uma abordagem mais sutil, em que os indivíduos podem escolher apenas determinados tipos de processamento ou coleta de apenas certos tipos de dispositivos.

Por último, quando consideramos a potencial penetração dos sistemas de IoT e a grande variedade de usos e abusos potenciais que pode acontecer com tais sistemas, as considerações de segurança se tornam mais importantes na lista de questões a serem abordadas de maneira efetiva e sistêmica por empresas e governos responsáveis. Neste sentido, significativamente, Weber (2015) ressalta que, uma vez que vários processos heterogêneos estão envolvidos no desenho, implementação e manutenção de sistemas de IoT, a preservação de segurança e privacidade depende da busca e implementação de quatro objetivos fundamentais:

1. resiliência a ataques para que o sistema evite pontos únicos de falha;
2. autenticação de dados;
3. controle de acesso aos dados fornecidos;
4. privacidade substancial, incluindo a anonimização de dados, para evitar – ou pelo menos tornar muito difícil – extrair inferências processando dados pessoais sem o consentimento do titular de dados.[48]

Esses objetivos devem ser perseguidos, tendo em mente que, em um ambiente de IoT, não existem aparelhos 100% seguros e todos os indivíduos se tornam potencialmente vulneráveis. Portanto, a melhor maneira de mitigar riscos é educar os indivíduos sobre seus direitos, seus papéis e responsabilidades na era digital. É somente por meio da colaboração e sinergia que os atores públicos e privados e as sociedades civis poderão enfrentar os desafios apresentados pela IoT, maximizar seus benefícios e evitar riscos, desencadeando assim uma verdadeira IoT humana e responsável.

A human rights perspective to decrypt the rise of the Internet of Things (IoT)

Abstract: The Internet of Things (IoT) is a phenomenon announced by its proponents as a true propellant of the next industrial revolution, able to generate considerable gains in terms of efficiency and growth. However, together with the benefits that the IoT can unleash, it seems necessary to evaluate the consequences that such phenomenon can deploy on the full enjoyment of Fundamental Huma Rights. The purpose of this article is, therefore, to briefly investigate what technological evolutions are driving

[48] Ver Weber (2015, p. 621).

– and being enabled by – the IoT, what could be the impact of the IoT on individuals' rights. The article analyses what elements could allow public and private stakeholder to face the challenges of the IoT, while facilitating, in synergy, the development of responsible IoT systems, in compliance with United Nations Guiding Principles on Business and Human Rights. First, this paper will analyse the IoT phenomenon, stressing the intimate link between the IoT and the Big Data and Artificial Intelligence phenomena. The second section will briefly scrutinise the impact that the aforementioned phenomena may have on the full enjoyment of Fundamental Human Rights, providing some concrete examples. The concluding section will provide some suggestions on how states and businesses can implement the Principles effectively.

Keywords: Internet of Things. IoT. Big data. Artificial intelligence. Privacy. Security. UN Guiding Principles on Business and Human Rights.

Referências

AMIGO, I. The Metro Stations of São Paulo That Read Your Face. *Citylab*, 8 maio 2018. Disponível em: https://www.citylab.com/design/2018/05/the-metro-stations-of-sao-paulo-that-read-your-face/559811/.

ANGWIN, J.; LARSON, J.; MATTU S.; KIRCHNER, L. Machine Bias. *Propublica*, 23 maio 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

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

BASTONE N. Google says the built-in microphone it never told Nest users about was 'never supposed to be a secret'. *Business Insider*, 20 fev. 2019. Disponível em: https://www.businessinsider.nl/nest-microphone-was-never-supposed-to-be-a-secret-2019-2/?international=true&r=US.

BELLI, L.; DE FILIPPI, P.; ZINGALES, N. (Org.). Recommendations on Terms of Service & Human Rights. *United Nations Internet Governance Forum*, 2015. Disponível em: https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/830-dcpr-2015-output-document-1/file.

BELLI, L.; SCHWARTZ, M.; LOUZADA, L. Selling your Soul while Negotiating the Conditions: From Notice and Consent to Data Control by Design. *Health and Technology Journal*, v. 7, n. 4, p. 453-467, 2017. Disponível em: http://link.springer.com/content/pdf/10.1007%2Fs12553-017-0185-3.pdf.

BNDES. *Relatório do plano de ação*. Iniciativas e projetos mobilizadores. 2017. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil.

CALO, R. M. Against Notice Skepticism in Privacy (and Elsewhere). *Notre Dame L. Rev.*, 87, 1027, 2013. Disponível em: https://digitalcommons.law.uw.edu/faculty-articles/29.

CISCO. *At a glance*: internet of things. 2016. Disponível em: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf.

DAY, M. Your smart light can tell Amazon and Google when you go to bed. *Bloomberg Technology*, 12 fev. 2019. Disponível em: https://www.bloomberg.com/news/articles/2019-02-12/your-smart-light-can-tell-amazon-and-google-when-you-go-to-bed.

EUROPEAN COMMISSION. *Report on the Consultation on IoT Governance*. 2013. Disponível em: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746

FEHRENBACHER, K. How Tesla is ushering in the age of the learning car. *Fortune*, 16 out. 2015. Disponível em: https://fortune.com/2015/10/16/how-tesla-autopilot-learns/.

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

GARTNER. *Gartner says the Internet of Things will transform the data center*, 19 mar. 2014. Disponível em: http://www.gartner.com/newsroom/id/2684616.

GARVIE, C.; BEDOYA, A. M.; FRANKLE J. The perpetual line-up. Unregulated Police Face Recognition in America. *Georgetown Law – Center on Privacy & Technology*, 2016. Disponível em: https://www.perpetuallineup.org/.

GREENLEAF, G. Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018. *UNSW Law Research Paper*, n. 18-56, maio 2018. Disponível em: https://ssrn.com/abstract=318454.

GSMA. *Unlocking the Value of IoT through Big Data*. Version 1.0. 2015. Disponível em: https://www.gsma.com/iot/wp-content/uploads/2015/12/cl_iot_bigdata_11_15-004.pdf.

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

HOWARD, P. N. *Pax Technica*: How the Internet of Things May Set Us Free or Lock Us Up, by writer and professor of communication. New Haven: Yale University Press, 2015.

HUMAN RIGHTS COUNCIL. Human Rights and Transnational Corporations and Other Business Enterprises. *Resolution 17/4 of 16 June 2011*. 6 jul. 2011. Disponível em: https://www.ohchr.org/EN/Issues/Business/Pages/ResolutionsDecisions.aspx.

ICO – INFORMATION COMMISSIONER'S OFFICE. *Big data, artificial intelligence, machine learning and data protection*. [s.l.]: [s.n.], 2017.

IOT ANALYTICS. *State of the IoT 2018*: Number of IoT devices now at 7B – Market accelerating. 8 ago. 2018. Disponível em: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

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

ITU – INTERNATIONAL TELECOMMUNICATION UNION. *The Internet of Things*. ITU Internet Reports. Geneva: ITU, 2005.

JESUS JUNIOR, Airton A. de; MORENO, Edward David. Segurança em infraestrutura para internet das coisas. *Revista Gestão.Org*, v. 13, 2015. Edição Especial.

LESWING, K. A massive cyberattack knocked out major websites across the internet. *Business Insider*, 21 out. 2016. Disponível em: https://www.businessinsider.com/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10.

MACHULAK, M. P.; MALER, E. L.; CATALANO, D.; VAN MOORSEL, A. User-managed access to web resources. *In*: 6th ACM WORKSHOP ON DIGITAL IDENTITY MANAGEMENT. *Proceedings*... [s.l.]: ACM, 2010.

MADDOX, T. Cisco: The Internet of Everything is at tipping point. *TechRepublic*, 18 fev. 2018. Disponível em: https://www.techrepublic.com/article/cisco-the-internet-of-everything-is-at-tipping-point/.

MAGRANI E. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018.

MEIRA, S. Sinais do futuro imediato, #1: internet das coisas. *Ikewai*, Recife, 2016. Disponível em: http://boletim.de/silvio/sinais-do-futuro-imediato-1-internet-das-coisas/.

MILLER, C.; VALASEK, C. *Remote Exploitation of an Unaltered Passenger Vehicle*. 10 ago. 2015. Disponível em: www.illmatics.com/Remote%20Car%20Hacking.pdf.

MILLER, J. City of London calls halt to smartphone tracking bins. *BBC*, 12 ago. 2013. Disponível em: https://www.bbc.com/news/technology-23665490.

NG, A. Amazon will stop selling connected toy filled with security issues. *Cnet*, 5 jun. 2018. Disponível em: https://www.cnet.com/news/amazon-will-stop-selling-connected-toy-cloud-pets-filled-with-security-issues/.

NOBLE, S. *Algorithms of Oppression*: How Search Engines Reinforce Racism. New York: New York University Press, 2018.

NOURA, M.; ATIQUZZAMAN, M.; GAEDKE, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Networks and Applications*, v. 24, issue 3, p. 796-809, jun. 2019. Disponível em: https://doi.org/10.1007/s11036-018-1089-9.

O'NEIL, C. *Weapons of Math Destruction*: How Big Data Increases Inequality and Threatens Democracy. New York: Broadway Books, 2016.

PASQUALE F. *The Black Box Society* – The Secret Algorithms That Control Money and Information. Cambridge and London: Harvard University Press, 2015.

PRIVACY INTERNATIONAL. *IoT*. ([s.d.]). Disponível em: https://privacyinternational.org/types-abuse/iot.

PRIVACY INTERNATIONAL. *The police can use IMSI catchers to track your phone, and even intercept your calls and messages*. 15 fev. 2019. Disponível em: https://privacyinternational.org/feature/2729/police-can-use-imsi-catchers-track-your-phone-and-even-intercept-your-calls-and.

REN, J. *et al.* Information Exposure From Consumer IoT Devices. A Multidimensional, Network-Informed Measurement Approach. *IMC '19*, Amsterdam, out. 2019. Disponível em: https://doi.org/10.1145/3355369.3355577.

SCHIDER, C. A. Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age. *Denver Law Review*, v. 96, 2018.

SICARI, S.; RIZZARDI, A.; GRIECO, L. A.; COEN-PORISINI, A. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 2015.

SOLOVE, D. J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, v. 126, p. 1879-1880, 2013. Disponível em: https://pdfs.semanticscholar.org/809c/bef85855e4c5333af40740fe532ac4b496d2.pdf.

WEBER, R. H. Internet of things: Privacy issues revisited. *Computer Law & Security review*, v. 31, 2015.

ZUBOFF, S. *The Age of Surveillance Capitalism*: The Fight for a Human Future at the New Frontier of Power. London: Public Affairs, 2019.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

BELLI, Luca. Uma perspectiva de direitos humanos para decriptar a ascensão da Internet das Coisas (IoT). *Direitos Fundamentais & Justiça,* Belo Horizonte, ano 13, n. 41, p. 157-181, jul./dez. 2019.

Recebido em: 01.08.2019
Pareceres: 23.09.2019, 24.09.2019, 14.11.2019
Aceito para publicação em: 14.11.2019