Internet das Coisas, inovação e desafios: oportunidades, riscos e o papel do Estado em sociedades datificadas

Sivaldo Pereira da Silva
Vivian Peron

Resumo

A expansão da Internet das Coisas (IoT), com infraestrutura de sensores e dispositivos conectados que absorvem e processam dados, tem transformado espaços físicos em fontes de produção e captação informação. Neste cenário, o principal objetivo deste artigo é caracterizar como sistemas de IoT são uma forma inovadora de datificação da vida que abre oportunidades e riscos, apontando qual do papel do Estado nesse fenômeno emergente. Constatou-se que o Estado tem diante de si desafios significativos para criar normas que equilibrem proteção de direitos e estímulo à inovação neste campo, além de garantir infraestrutura tecnológica necessária. Modelos regulatórios multissetoriais são recomendados para lidar com as tensões entre o potencial transformador da IoT e os riscos de ampliação de ataques, vigilância e controle.

Abstract

The expansion of the Internet of Things (IoT), with its infrastructure of sensors and connected devices that capture and process data, has transformed physical spaces into sources of information production and collection. In this context, the primary objective of this article is to charac-

terize how IoT systems represent an innovative form of life datification that creates both opportunities and risks, highlighting the role of the State in this emerging phenomenon. It was found that the State faces significant challenges in creating regulations that balance the protection of rights with the promotion of innovation in this field, in addition to ensuring the necessary technological infrastructure. Multisectoral regulatory models are recommended to address the tensions between the transformative potential of IoT and the risks of increased attacks, surveillance, and control.

1. Introdução

Um dos pilares das inovações tecnológicas deste século é o exponencial aumento da produção e disponibilização de dados. Este fenômeno está intimamente ligado ao processo de *datificação* da vida, marcado pela difusão de aparelhos conectados que passaram a compor o ecossistema social e o tecido cultural contemporâneo. Isso vem se consolidando através do alargamento gradual de infraestruturas e microestruturas interligadas, composta por camadas físicas e lógicas. Capilarizadas no cotidiano, as pontas desse sistema são aquilo que nos é mais visível, apresentando-se na forma de dispositivos sociotécnicos como celulares, aplicativos, computadores, câmeras, wi-fi e conexões 5G.

A Internet das Coisas (Internet of Things – IoT) consiste na expansão deste cenário. Implica em um substancial fortalecimento da infraestrutura de *datificação* através da presença intensificada de máquinas e objetos conectados. Nestas primeiras décadas do século XXI isso está em fase de florescimento e a sua evolução ampliará enormemente a capacidade humana de compreender o mundo e, por consequência, de agir sobre este. Não apenas sobre o mundo natural, mas também sobre a vida social e, em última instância, permitirá compreender mais sobre o indivíduo enquanto unidade comportamental integrado a modelos estatísticos descritivos e preditivo avançados.

Muito mais que o exemplo banal de uma geladeira capaz de se conectar com os produtos e avisar quando algum deles está prestes a acabar, o que concretamente é relevante na concepção de Internet das Coisas é a sua capacidade de *datificar* o mundo. O que importa não é o que a geladeira faz, mas o que a geladeira apreende em termos de informação e aprende com nosso comportamento e como essa informação é processada, utilizada e, principalmente, como isso nos é devolvido. O que faz a geladeira parecer inteligente é a sua capacidade em se comunicar como se estivesse no mesmo nível cognitivo e emocional que o nosso e, para isso, requer captar dados, abrir-se sensitivamente para tal.

Não por acaso, um dos elementos centrais da IoT são os sensores. Onde estão? O que captam? Como armazenam e processam dados? Quais dados? Para quais finalidades? E quem são seus detentores? Sobretudo, o uso em larga escala de sensores é capaz de captar um amplo leque de informação e converter espaços físicos antes vazios em câmaras de produção de dados. Como isso pode significar um ganho de conhecimento com impactos positivos, ajudando a melhorar e baratear processos, prevendo catástrofe, otimizando serviços públicos, agilizando a resolução de crises, tornando a vida mais confortável etc. Ao mesmo tempo, é preciso discutir como o funcionamento desta infraestrutura pode também ampliar violações de direitos, inviabilizar a noção de privacidade e criar problemas de segurança pública.

Tendo como premissa que o processo de *datificação* é uma força vital que se assemelha ao *Zeitgeist* do século XXI e significa um salto epistemológico importante, considera-se necessário debater seus rumos, estabelecer seus princípios e limites. Pressupõe-se, nestes termos, que tal fenômeno requer a ação direta do Estado por implicar no manuseio de recursos estratégicos (dados) com potencial benefício público e, ao mesmo tempo, por ampliar o leque de ameças à segurança pública ou violação de direitos individuais e coletivos. Diante disso, o principal objetivo deste artigo é caracterizar como sistemas de IoT são uma forma inovadora de *datificação* da vida que abre oportunidades e riscos, apontando qual do papel do Estado nesse fenômeno emergente.

Assim, artigo segue dividido em três seções subsequentes.Primeiramente, será configurado um quadro conceitual e prático sobre o que é e como funciona IoT, apontando para os tipos de inovação e oportunidades que este fenômeno implica. Na seção seguinte, serão identificadas as fragilidades inerentes aos dispositivos e sistemas de IoT, seus problemas e riscos, sobretudo no tocante à violação de direitos e segurança. Por fim, a última seção será dedicada a configurar o papel do Estado no estabelecimento políticas digitais promissoras capazes de lidar com as oportunidades e riscos gerados por estes sistemas.

2. Internet das Coisas: inovação, infraestrutura e funcionamento

Para compreendermos de modo mais consistente como funcionam a IoT convém, primeiramente, fazermos um paralelo com a Internet convencional, tal como a conhecemos e apontar diferenças. A Internet nasce incialmente como uma pequena rede de computadores de médio porte; ampliou-se posteriormente deixando de ser restrita e ao incluir computadores pessoais; e expandiu-se ainda mais ao incorporar aparelhos computacionais portáteis (como *smartphones, tablets* e afins) conectados por protocolos comuns através do qual se trafega conteúdos multimidias gerados por indivíduos ou organizações.

A Internet das Coisas (IoT) parte deste mesmo modelo básico de máquinas conectadas trafegando informação em rede, porém com três inovações importantes: (1) aquilo que é conectado passa a ser também todos os tipos de máquinas e outros objetos; (2) o fluxo de informação e comunicação deixa de ser centrado em indivíduos e organizações e passa a incorporar outras máquinas e objetos que se comportam como entes ativos formando um ecossistema de informação híbrido; (3) e, por fim, o que é colocado em rede vai aquém e além de conteúdo multimídia como texto, som ou imagem. Aquém porque boa parte dos dados de *input* que trafegam em IoT são unidades extremamente básicas e primárias de informação que buscam representar o mundo a partir de seus

indicadores mínimos. E vai além porque esta captação de dados ganha a escala de milhões e bilhões de *Gi`gabits* com amplitude e granulação, conseguindo assim descrever eventos em detalhes e desenvolver modelos estatísticos robustos.

Neste sentido, quando falamos de IoT estamos falando de uma rede microestruturas e infraestruturas que captam e processam quantidades inéditas e volumosas de informação capazes de potencializar o conhecimento sobre o mundo. Esta cadeia é extremamente relevante pois nos ajuda a vislumbrar na prática como os sistemas de IoT operam; como se caracterizam; onde estão suas fragilidades e como podem ser inovadoras. Portanto, quando falamos de IoT não devemos pensar no objeto ou no aparelho conectado e sim na cadeia de dispositivos e infraestrutura que conectam esse aparelho.

Muitos autores se propõem a explicar o funcionamento da IoT a partir da concepção de camadas (ATTIA, 2019; MISHRA; PAUL, 2020; SHACKELFORD, 2020; GREENGARD, 2021; KOPETZ; STEINER, 2022; CHIARA, 2022). Para efeito deste artigo e levando em conta essas diversas contribuições, consideramos útil explicar tais camadas nomeando-as por tipos de ação assumida, posicionada na cadeia de *datificação* dos sistemas de IoT. Neste sentido, podemos identificar seis camadas fundamentais: (1) Captação; (2) Leitura; (3) Conexão; (5) Transporte; (6) Armazenamento e (7) Processamento.

As primeiras camadas dos sistemas de IoT são aquelas nas quais residem os elementos mais originais e que carregam o sentido de inovação das coisas conectadas. A camada de captação é composta por sensores e *tags* e se configuram como um sistema de entrada de dados possibilitando a primeira ação de *datificação*: a identificação. Para produzir conhecimento sobre algo (e eventualmente ter poder sobre isso) precisamos identificá-lo, minimamente. Neste processo, os elementos de identificação dos objetos podem ser *tags* que não são máquinas e não funcionam com base energética, mas tem a função primordial de servir como marcador acoplado ao objeto que será mapeado e conectado por leitores. Podem ser também sensores que operam com alguma

forma de energia subjacente, sendo ativos no processo de comunicação ao emitir sinais para outros objetos ou sensores em seu raio de atuação. Por exemplo, etiquetas de RFID são dispositivos de identificação que contêm um código eletrônico associado a um objeto físico. Estas etiquetas podem ser passivas ou ativas. Os RFIDs passivos não possuem fonte de energia própria e são acionadas por campo elétrico emitido por um leitor RFID. Já as etiquetas ativas são microdispositivos com fonte de energia própria, que permite ações mais avançadas, transmitindo sinais a distâncias maiores e integrando sensores (TZAFESTAS, 2018; KOPETZ; STEINER, 2022).

Geralmente, os sensores são estruturas extremamente simplificadas e por isso operam com baixíssimos níveis energéticos. Seja através de *tags* ou sensores, a identificação é apenas a primeira etapa deste processo de datificação. A segunda camada é responsável pela leitura. Os leitores são instrumentos voltados para perceber e registrar dados de embutidos *tags* ou emitidos por sensores (RDIF, *blue tooth*). Os leitores rastreiam, mapeiam, captam e decodificam dados brutos e primários. Na prática, são estruturas que operam nesta cadeia recebendo e organizando os fluxos de dados em primeira instância. Na terceira camada, temos os conectores que são infraestruturas de comunicação sem fio que possibilitam o rápido fluxo desses dados coletados para um primeiro estágio de armazenamento e processamento em estações mais próximas. São as redes sem fio como wif-fi, 4G, 5G e 6G. Na quarta e quinta camada os dados atingem a infraestrutura de transporte de longa distância da internet constituída por *backhauls* e *backbones*, marinhos e terrestres (SILVA; BIONDI, 2012; TANCZER et al, 2019; YOO, 2019) além de *datacenters* na camada de armazenamento e processamento onde operam computação em nuvem ou *edge computing* (computação de borda).

Na prática, toda a infraestrutura de IoT e suas camadas fortalecem uma de computação ubíqua onde tudo pode ser registrado e analisado ampliando enormemente a capacidade de conhecer eventos. Do ponto de vista da inovação de processos, isso traz, naturalmente, diversos benefícios que podemos sintetizar nos seguintes termos:

a) Monitoramento – Sistemas de IoT transformam ambientes e objetos antes inertes em valores estatísticos ou, visto por outro ângulo, como entes que produzem dados. Isso permite um robusto sistema de acompanhamento de processos, *insights* em tempo real e, em última instância, maior controle.

b) Operacionalização – A IoT permite melhor eficiência no funcionamento de máquinas. sistemas de objetos e sistemas de ações humanas. Sobretudo por que produzem informações que permitem tornar operações menos susceptíveis a erros cujo resultado é uma melhoria no desempenho de sistemas existentes, mas também novas características incluindo algumas que ainda inexistentes (GREENGARD, 2021). Neste sentido, para Kopetz e Steiner (2022) isso significa forças inovadoras que influenciam a criação de novos mercados e a produtividade em diversos setores:

> We distinguish between *technology push* and *technology pull* forces. The *technology push forces* see in the IoT the possibility of vast new markets for novel ICT products and services, while the *technology pull forces* see the potential of the IoT to increase the productivity in many sectors of the economy (KOPETZ; STEINER, 2022, p. 325)

c) Impactos econômicos – Esse monitoramento constante aliado à otimização operacional tem um efeito econômico relevante uma vez que possibilita melhor utilização de recursos evitando perdas bem como prejuízos decorrentes do mal funcionamento de sistemas e máquinas (NICOLESCU et al, 2018; MAGRANI, 2018; ATTIA, 2019; VOULGARIDIS et al. 2022). Isso não está apenas restrito a grandes organizações:

> The Internet contributes to increased productivity in large companies and it is even more important for small and medium-sized enterprises and start-ups. There was a survey involving 4,800 SMEs in 12 countries. And it was found that the enterprises using Internet technology,

> increased revenue twice as fast as businesses with minimal use of the Internet of Things. These results can be applied to all economy sectors (KARLOV et al 2019, p. 8).

d) Intensificação da Automação – IoT facilita a automação de várias tarefas diárias, conectando dispositivos que podem trabalhar em conjunto sem a necessidade de intervenção manual. Isso tem uma relação direta com o desenvolvimento de sistemas de Inteligência Artificial atuando em diversos setores e de forma localizada:

Cada vez mais dispositivos digitais são capazes de processar tarefas localmente. Os dados são transmitidos a partir de sensores em um dispositivo, como um robô ou veículo autônomo. Enquanto o sistema de IA de borda realiza os cálculos, ele armazena os resultados no próprio dispositivo. Em alguns casos, esses dados podem ser enviados para a nuvem. Esse modelo permite que os dispositivos operem de forma mais rápida, inteligente e com menor consumo de energia. Isso muda radicalmente o modo como as máquinas autônomas funcionam e prolonga a vida útil das baterias dos sensores por anos (GREENGARD, 2021, p. 40)[4]

e) Prevenção e mitigação – Sistemas de IoT têm implicações diretas na predição e tratamento de problemas que envolvem saúde pública, emergências sociais ou catástrofes. Diversos sensores estão sendo desenvolvidos e testados para conectar o corpo humano em tempo real e produzir informações biológicas que serão fundamentais para prevenção e tratamento de doenças. Dispositivos interconectados criam uma nova fronteira para a interação entre medicina e paciente. A expressão Internet of Body (IoB) enfatiza este campo emergente (LEENES et al 2018). Para além do corpo, sensores encravados no meio ambiente criam redes de proteção e mitigação de eventos ambientes com potencial dano coletivo (SHACKELFORD, 2020).

4 Tradução própria do original em inglês.

Como vimos, do ponto de vista histórico, significa falarmos em um potencial *turn point* epistemológico. Do ponto de vista sociotécnico, implica em pensarmos em uma ampliação da infraestrutura e do aparato de vigilância e *dataveillance* (DIJCK, 2014). Por isso, qualquer conceito mais consistente de IoT deve se ater ao caráter de rede massiva de sensores embutidos nas coisas, nos ambientes e nas práticas culturais e toda a sua cadeia de transporte e processamento de dados em larga escala e suas conequências.

3. Fragilidades, problemas e riscos

Sistemas de IoT tendem a ser ubíquos atuando na captação massiva de dados e possibilitando o gerenciamento de bens e serviços de bilhões de usuários. Por isso, o fluxo de dados precisa ser constante e confiável e suas falhas podem ter um largo espectro de consequências que vão desde inconvenientes mais simples até impactos mais graves, com possibilidade de colocar vidas em risco (GREENGARD, 2021; SHACKELFORD, 2020; TZAFESTAS, 2018). Na prática, dispositivos de IoT são bem mais vulneráveis a ataques justamente por serem, na ponta, extremamente simplificados, operando com baixíssimo nível energético, e, por isso, com baixa capacidade de operar recursos de segurança. Paralelamente a isso, há a questão da escala de introdução dos dispositivos de IoT no cotidiano (SHACKELFORD, 2020). Com o crescente uso de IoT em diversas atividades humanas, envolvendo serviços e produtos utilizados por grande volume de pessoas, a conjunção entre vulnerabilidade a ataque e impacto demográfico se torna um problema especialmente importante. Se por um lado um ataque cibernético em dispositivos tradicionais tem um efeito individual e isolado (por exemplo, em um computador, ou celular), por outro lado, um ataque a uma rede de dispositivos de IoT pode ser especialmente crítico pois operam em uma escala muito maior cuja dimensão é coletiva.

Neste sentido cada uma das camadas da cadeia dos sistemas de IoT podem sofrer diferentes tipos de ataques. Podemos aglutinar os riscos

quanto à segurança de sistemas de IoT em 4 categorias mais relevantes: (a) ataques de funcionamento; (b) ataques de comunicação; (c) ataques de identificação; (d) ataques de invasão. Convém sintetizar como cada tipo de problemas de segurança se caracterizam e seus efeitos.

Os ataques de funcionamento são aqueles que visam inviabilizar a operação do dispositivo, tornando-o inativo. Um bom exemplo são os chamados "ataque de privação de sono" (*sleep deprivation attack*). O objetivo é inviabilizar energeticamente o funcionamento de dispositivos de uma rede impedindo-os de economizar energia, tendo em vista se caráter diminuto especialmente na camada de captação. Os dispositivos são assim programados para "hibernar" e assim economizar recursos energéticos. Este tipo de ataque impede que haja essas pausas mantendo -os continuamente ativos, o que resulta em um rápido esgotamento da energia e, consequentemente, no seu desligamento (KHAN; SALAH, 2018).

No caso de ataques de comunicação, a ação se dá na camada de transporte de dados nas redes sem fio. Um exemplo é o ataque baseada em interferência de sinal de rádio (*Jamming Adversaries*) quando um agente emite sinais clandestinos de rádio bombardeando os equipamentos que passam a ficar sobrecarregados impedindo-os de se comunicar com outros artefatos regulares da rede. No nível mais básico pode degradar o fluxo de comunicação tornando o transporte de dados mais lento. No nível mais alto, pode impedir a comunicação bloqueando o transporte de dados, isolando sensores e dispositivos da rede (MISHRA; PAUL, 2020).

Já os ataques de identificação estão baseados em uma importante característica dos sistemas de IoT que é o reconhecimento de objetos como entes únicos assumindo determinados papeis na rede. Um bom exemplo são os denominados ataques *Sybil* quando um invasor insere na rede identidades falsas de objetos ou sensores, possibilitando-o assim de controlar a inserção de dados e assumir o fluxo de informação, manipulando-o. Em um cenário industrial, por exemplo, um invasor poderia inserir identidades falsas em uma rede de sensores, produzindo dados incorretos sobre temperatura e umidade e fazendo com que as máqui-

nas funcionem a partir de parâmetros distorcidos e inexistentes (KHAN e SALAH, 2018). Ataques de identificação também podem ocorrer no nível físico, por exemplo, ao se vincular um objeto falsificado a uma etiqueta legítima quebrando assim o vínculo entre objeto físico e seu representante digital (KOPETZ; STEINER, 2022).

Quanto aos ataques de captura estes ocorrem quando objetos da rede se tornam porta de entrada para que usuários não autorizados tenham acesso aos dados armazenados ou transportados, quebrando a privacidade do sistema. Invasores podem usar *scripts* maliciosos ou *sniffers* para capturar a ID de uma sessão e, assim, assumir o controle da sessão. Com isso, obtêm acesso não autorizado ao servidor, podendo explorar informações privadas (MISHRA; PAUL, 2020). Além disso, as interfaces de aplicativos que conectam dispositivos IoT (incluindo *middlewares*) são particularmente simplificadas devido à própria estrutura do *hardware* nos quais são baseadas, o que impossibilita a instalação de sistemas mais robustos de segurança tornando esses dispositivos mais susceptíveis a invasões.

4. IoT, datificação e o papel do Estado

O estabelecimento de objetos conectados agindo em larga escala em ambientes físicos e sociais, formando uma intensa rede de coleta de dados ubíqua, significa não apenas um maior aporte de conhecimento e controle sobre o mundo, mas sobretudo, a ampliação do processo de *datificação* da vida através do qual tudo passa a ser monitorado, medido e controlado através do intenso fluxo de diferentes tipos de dados. Se por um lado temos um grande potencial na implantação de sistemas de IoT capazes de gerar avanços significativos na performance de diversas atividades, com horizonte de novos serviços, produtos e produção de conhecimento capaz de prevenir e propor soluções, por outro lado, a proliferação de objetos conectados podem ser tornar parte do cotidiano e ampliar os problemas de segurança e privacidade, criando novas formas de violação e colocando sistemas, bens públicos e vidas em risco.

Neste cenário, o Estado enfrenta grandes desafios regulatórios e de governança devido às características inovadoras inerentes a esse processo de *datificação* gerado pela intensificação dos dispositivos de IoT. Primeiramente, trata-se de um setor expansivo de rápida evolução e transversal. Qualquer regulação ou política pública precisa levar em conta essa velocidade, diversidade e amplitude, que coloca normas em constante tensão para lidar com diferentes contextos de usos. Segundo, essa diversidade setorial tende a gerar uma fragmentação normativa capazes de dificultar o estabelecimento de padrões universais de segurança e privacidade e estabelecer ações unificadas contra problemas de larga escala. Terceiro, a proliferação de dispositivos conectados requer interoperabilidade e isso só pode ser definido a partir de normas comuns, cabendo ao Estado consolidá-las, levando em conta os diferentes interesses dos diferentes *players* nas diversas camadas da cadeia de IoT. Quarto, há uma clara tensão entre violação de direitos e inovação técnica na qual especialistas, organizações civis e ativistas reivindicam legislações mais protetivas contra o poder e a ubiquidade destas estruturas e, do outro lado, setores econômicos reivindicam regulação menos densa sob o argumento de que o excesso de normas pode gerar inibição do potencial inovador do setor. Quinto, as estruturas regulatórias existentes muitas vezes não são adequadas para lidar com os desafios específicos da IoT, como identificadores únicos, redes distribuídas, coleta massiva de dados sem consentimento individualizado. Sexto, para funcionar, IoT pressupõe não apenas microestruturas de sensores mas infraestruturas de transporte (como *backbones, backauls*, 5G, 6G), de tráfego (como Pontos de Troca de Tráfego – TTs) e de armazenamento de dados (como *datacenters*) que tendem a se constituir como um gargalo para muitos países devido à forte dependência tecnológica.

Todos esses desafios requerem amplos esforços em diversas frentes exigindo que o Estado opere diferentes papeis concomitantes: como regulador na definição de regras e padrões deontológicos; como indutor no fomento à criação de infraestruturas e *expertise* técnica; e como protetor de direitos baseado em princípios de interesse público.

Em seu papel de regulador o Estado precisa estabelecer limites e normas de conformidade quanto à segurança que dispositivos de IoT devem sustentar. Neste sentido, o conceito de "privacidade por *design*" é um bom exemplo de como o Estado pode agir introjetando normas de proteção por natureza replicáveis que acompanhe a escala dos sistemas de IoT. Ou seja, uma forma de gerar efeitos transversais para lidar com a ubiquidade dos dispositivos de IoT, garantindo que carreguem mecanismos anti-violação. Uma outra dimensão neste papel é garantir a interoperabilidade entre dispositivos de diferentes fabricantes e garantir que esses padrões sejam abertos e pactuados. Este elemento regulador é essencial pois viabiliza que um ecossistema robusto floresça com diversidade de dispositivos operando de forma intercambiável, evitando oligopólios ou monopólios econômicos, incentivando potenciais inovações técnicas.

Como indutor, o Estado tem como principal papel garantir a existência de uma infraestrutura capaz de suportar e fazer funcionar sistemas de IoT. O volume de dados processados está em expansão com a conexão de mais dispositivos e o surgimento de sistemas de IA. Para suportar tais demandas, é necessário que haja toda uma infraestrutura de base que requer grandes investimentos (VINUEZA-MARTÍNEZ, 2018; FANOU, et al., 2020). Principalmente porque sistemas de IoT funcionam mediante a existência de nuvens de dados. Embora a expressão "nuvem" possa soar abstrata, trata-se de uma metáfora para a conjunção de infraestrutura materiais e lógicas de transporte, armazenamento e processamento de dados de longa distância e curta distância. "As nuvens são cruciais para a IoT porque, entre outras coisas, fornecem um ambiente altamente escalável para armazenamento de dados [...] " (GREENGARD, 2021, p. 74).

Isso também envolve políticas públicas que promovem a integração da IoT em infraestruturas locais como cidades inteligentes e seus equipamentos. Ao mesmo tempo que precisa fomentar infraestruturas, o Estado também precisa olhar para as microestruturas pois nelas estão boa parte dos problemas de segurança que envolvem IoT. O problema da escala aliado à busca por diminuição dos custos desses dispositivos requer que o Estado crie mecanismos para subsidiar e fomentar o de-

senvolvimento de inovações de segurança, capazes de lidar com o problema do custo que isso envolve e ao mesmo tempo solucionar que aumente a segurança da rede.

Por fim, o papel de proteção de direitos requer não apenas um Estado forte mas também um ecossistema de governança ativo e representativo. Neste caminho, ações de regulação tradicional, mesclada com mecanismos de corregulação e principalmente modelos de governança multissetorial (que incorpora institucionalmente diversos segmentos sociais como governo, organizações sociais, empresas, pesquisadores, especialistas etc.) são mecanismos adequados para lidar com as complexidades e os desafios específicos da IoT (Weber, 2013; Jacobs, 2020a. 2020b). Para isso, entes reguladores devem ser estabelecidos com capacidade de *enforcenment* e capacidade técnica para auditar e monitorar as ações destas redes em sua expansão.

Considerações finais

Este artigo discutiu como IoT é hoje um fenômeno com forte viés inovador quanto à ampliação dos processos de *datificação* da vida, criando oportunidades e riscos. Primeiramente, observou-se que sistemas de IoT são redes que constituídas por camadas que envolvem captação, leitura, conexão, transporte, armazenamento e processamento de dados, funcionando através de microestruturas e infraestruturas capazes de potencializar o conhecimento sobre o mundo. Isso permite monitoramento detalhado, operacionalização eficiente e automação de processos, reduzindo erros e aumentando o desempenho de sistemas. A IoT também traz impactos econômicos relevantes ao elevar a produtividade e diminuir custo. Amplia a criação e manutenção de sistemas de Inteligência Artificial (IA) e permite a prevenção e mitigação de crises e emergências coletivas.

Se por um lado, a Internet das Coisas pode significar um salto epistemológico e técnico relevante neste século, também implica em problemas decorrente de suas próprias características disruptivas. Cada ca-

mada pode trazer diferentes tipos de ações maliciosas como (a) ataques de funcionamento; (b) ataques de comunicação; (c) ataques de identificação e (d) ataques de captura. Tais riscos exigem a necessidade de medidas de segurança mais rigorosas pois trata-se de ataques que podem gerar danos em larga escala.

Nesse contexto, o Estado tem desafios complexos para criar normas que acompanhem a velocidade de evolução do setor, evitando a fragmentação normativa e garantindo interoperabilidade. Além disso, é necessário lidar com tensões entre proteção de direitos e inovação, estabelecendo modelos regulatórios multissetoriais capazes de lidar com esta dualidade.

A infraestrutura de suporte à IoT, incluindo sensores, redes e armazenamento de dados, representa outro desafio, especialmente para países com histórico de dependência tecnológica. Como indutor, o Estado deve incentivar e investir em infraestrutura de transporte e armazenamento de dados, tanto no nível local quanto nacional, visando a soberania do interesse público neste campo.

Embora haja em diversos países planos estratégicos e alguma regulação incipiente que versa sobre IoT, ainda não há um marco regulatório sistêmico capaz de lidar com as diversas camadas e dimensões do problema. Para os próximos anos, é preciso compreender que sistemas de IoT significam ampliação do conhecimento sobre o mundo e isso também implica em maior controle e poder. Cabe ao Estado direcionar essas forças inovadoras, fazendo com que o salto epistemológico propiciado por estas novas formas de produção de conhecimento se convertam em benefícios coletivos, ao invés da ampliação da vigilância e concentração de poder típico do processo de plataformização.

Referências

ATTIA, Tarek M. Challenges and Opportunities in the Future Applications of IoT Technology. **2nd Europe – Middle East – North African Regional Conference of the International Telecommunications Society (ITS):** Leveraging Technologies For Growth, Aswan, Egypt, 18th-21st February, 2019, International Telecommunications Society (ITS), Calgary, 2019.

CHIARA, Pier Giorgio. The IoT and the new EU cybersecurity regulatory landscape. **International Review of Law, Computers & Technology**, v. 36, n. 2, p. 118-137, 2022.

DIJCK, José van . 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society** 12 (2), p. 197-208, 2014.

FANOU, R. et al.. Unintended Consequences: Effects of Submarine Cable Deployment on Internet Routing. In: Sperotto, A., Dainotti, A., Stiller, B. (Org.) Passive and Active Measurement. PAM 2020. **Lecture Notes in Computer Science**, vol 12048. Cham: Springer, 2020.

GREENGARD, Samuel**. The Internet of Things**. Revised and updated edition. Cambridge: The MIT Press, 2021.

JACOBS, Naomi et al. Governance and Accountability in Internet of Things (IoT) Networks. In: YATES, Simeon J.; RICE, Ronald E. (Org.). **The Oxford Handbook of Digital Technology and Society**. Oxford: Oxford University Press, 2020b.

JACOBS, Naomi et al. Who trusts in the smart city? Transparency, governance, and the Internet of Things. **Data & Policy**, v. 2, 2020a.

KARLOV, Dmitriy et al. The implementation of the IoT concept in the post-industrial economy. **Revista Espacios**, v. 40, n. 38, p. 1-11, 2019.

KHAN, Minhaj Ahmad; SALAH, Khaled. IoT security: Review, blockchain solutions, and open challenges. **Future Generation Computer Systems**, v. 78, p. 964-979, 2018.

KOPETZ, Herman ; STEINER, Wilfried., W. Internet of Things. In: KOPETZ, H. ; STEINER, W. **Real-Time Systems. Springer**, Cham, 2022, p. 325-340.

LEENES, Ronald et al (Org.). **Data protection and privacy**: the internet of bodies. Portland: Hart Publishing, 2018.

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

MISHRA, Saumya; PAUL, Aditi. A critical analysis of attack detection schemes in IoT and open challenges. In: IEEE **International Conference on Computing, Power and Communication Technologies (GUCON),** Greater Noida, India. Anais, 2020.

NICOLESCU, R. et al. Mapping the Values of IoT. J**ournal of Information Technology**, 33 (4), 345-360, 2018.

SHACKELFORD, Scott J. **The internet of things:** what everyone needs to know. Nova York: Oxford University Press, 2020.

SILVA, Sivaldo Pereira da; BIONDI, Antonio (Org.). **Caminhos para a universalização da internet banda larga:** experiências internacionais e desafios brasileiros. 1. ed. São Paulo: Intervozes, 2012.

TANCZER, L. M. et al. The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V.Mohan (Org.). **Rewired:** Cybersecurity Governance. Hoboken: Wiley, 2019.

TZAFESTAS, Spyros G. Ethics and law in the Internet of Things world. **Smart Cities**, v. 1, p. 98-120, 2018.

VINUEZA-MARTÍNEZ, Jorge et al. A study of the Internet and connectivity in South American countries to 2017: An analytical perspective. **Revista Espacios**, v. 39, n. 16, p. 6, 2018.

VOULGARIDIS, Konstantinos et al. IoT and digital circular economy: Principles, applications, and challenges, **Computer Networks**, 219, 2022.

WEBER, Rolf H. Internet of things – Governance quo vadis? **Computer Law & Security Review,** v. 29, n. 4, p. 341-347, 2013.

YOO, C. S. . The Emerging Internet of Things: Opportunities and Challenges for Privacy and Security. In **Governing Cyberspace during a Crisis in Trust**: An essay series on the economic potential – and vulnerability – of transformative technologies and cyber security. Centre for International Governance Innovation, p. 41–44, 2019.

Sivaldo Pereira da Silva · Professor da Faculdade de Comunicação (FAC) e do Programa de Pós-Graduação em Comunicação da Universidade de Brasília (UnB). PhD em Comunicação e Cultura Contemporâneas pela Universidade Federal da Bahia (UFBa), com estágio doutoral na University of Washington (EUA). Possui pós-doutorado no Centro de Estudos Avançados em Democracia Digital e Governo Eletrônico (CEA-DD), UFBa. Foi pesquisador visitante no Instituto de Pesquisa Econômica Aplicada (IPEA); consultor da UNESCO e professor visitante na Technische Universität Dortmund (Alemanha). É fundador e coordenador do grupo de pesquisa Centro de Estudos em Comunicação, Tecnologia e Política (CTPol) e pesquisador do Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INCT-DD).

Vivian Peron · Doutora em Relações Internacionais pela Universidade de Brasília (UnB), com estágio doutoral no Massachusetts Institute of Technology (MIT), nos EUA. Mestrado em Comunicação Social pela Universidade Federal de Minas Gerais (UFMG). Tem pós-doutorado em Relações Internacionais pela Universidade de Brasília (UnB) e pós-Doutorado em Sociologia pela Universidade Federal de São Paulo (Unifesp). Foi pesquisadora no IPEA , consultora da UNESCO e professora no Departamento de Ciência Política e Relações Internacionais do Centro Universitário do Distrito Federal (UDF). Atualmente é coordenadora de Articulação Federativa do Laboratório de Cultura Digital (LabCD), projeto em parceria do Ministério da Cultura (MinC) e Universidade Federal do Paraná (UFPR), onde desenvolve pesquisa de pós-doutorado sobre estratégicas de comunicação e cultura digitais na implementação de políticas públicas governamentais.