Internet das Coisas no Brasil: estado da arte e reflexões críticas ao fenômeno

Eduardo Magrani
Doutor e mestre em Direito Constitucional e Teoria do Estado pela Pontifícia Universidade Católica do Rio de Janeiro. *Senior Fellow* na Universidade Humboldt de Berlim, no Alexander von Humboldt Institute for Internet and Society (HIIG). Coordenador do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Professor de Direito e Tecnologia e Propriedade Intelectual da FGV, IBMEC e PUC-Rio. Advogado atuante nos campos de Direitos Digitais, Direito Societário e Propriedade Intelectual. Autor de diversos livros e artigos na área de tecnologia e propriedade intelectual.

Resumo: A interação contínua entre dispositivos inteligentes, sensores e pessoas aponta para o número crescente de dados que são produzidos, armazenados e processados e alteram nosso cotidiano sob diversos aspectos. O contexto recente de Internet das Coisas (IoT) pode proporcionar benefícios econômicos ao Estado e a empresas, bem como comodidade aos consumidores. Em contrapartida, a crescente conectividade acarreta desafios significativos nas esferas de proteção da privacidade e segurança dos dados, tanto pessoais quanto profissionais. Este artigo aborda alguns desses desafios e organiza informações fundamentais para melhor entendimento sobre este cenário cada vez mais marcado pela hiperconectividade e que serve de base para a construção de um Plano Nacional de Internet das Coisas no Brasil.

Palavras-chave: Internet das Coisas; informação; tecnologia.

The Internet of Things in Brazil: state of the art and critic reflections on the phenomenon

Abstract: The continuous interaction between intelligent devices, sensors and people points to the increasing number of data that is produced, stored and processed and change

our daily lives in various aspects. The recent Internet of Things (IoT) context can provide economic benefits to the state and business, as well as convenience to consumers. On the other hand, increasing connectivity poses significant challenges in the areas of privacy and data security protection, both personal and professional. This article addresses some of these challenges and organizes key information for a better understanding of this scenario that is increasingly marked by hyperconnectivity and which serves as the basis for building an adequate Internet of Things in Brazil.

Keywords: Internet of Things; information; tecnology.

Introdução

A tecnologia está mudando rapidamente a maneira como interagimos com o mundo à nossa volta. A fim de atender às mais novas demandas de consumidores, empresas estão desenvolvendo produtos com interfaces tecnológicas e com componentes do cenário de Internet das Coisas que seriam inimagináveis há uma década.

Existem fortes divergências em relação ao conceito de Internet das Coisas (em inglês, *Internet of Things* – IoT),[1] e não há consenso sobre um que seja capaz de abarcar a complexidade sócio-técnica do fenômeno. O que as definições de IoT têm em comum é que se concentram em como computadores, sensores e objetos interagem uns com os outros e processam as informações/dados em um contexto de hiperconectividade.[2] De maneira geral, a IoT compreende um conjunto de objetos interconectados com a Internet e que cria um ecossistema de computação onipresente, com o objetivo de facilitar e trazer soluções a desafios cotidianos, a exemplo de soluções na área de saúde, mobilidade urbana e saneamento.

[1] É necessário salientar que a expressão *Internet das Coisas* se refere, basicamente, a objetos que contêm sensores conectados que captam e tratam informações. Tendo em vista a necessidade de despertarmos uma consciência (crítica) principalmente no público não especializado no tema, entende-se que, apesar de ser, de fato, menos técnica, essa nomenclatura atende melhor essa necessidade do que se pautarmos a abordagem nos conceitos técnicos de sensores e objetos rastreáveis.

[2] FTC STAFF REPORT, 2015.

Todos os dias, "coisas" com capacidade de compartilhar, processar, armazenar e analisar um volume enorme de dados entre si são conectadas à Internet. Esta prática é o que une a IoT ao conceito de *big data*; termo utilizado para descrever mecanismos de organização de grandes quantidades de dados estruturados, semiestruturados ou não estruturados[3] que potencialmente podem de ser explorados para obter informações.

A combinação entre objetos inteligentes[4] e *big data* alimenta um mercado lucrativo que irá alterar significativamente a maneira como vivemos.[5] Algumas pesquisas estimam que, em 2020, a quantidade de objetos interconectados passará dos 25 bilhões, podendo chegar a 50 bilhões de dispositivos inteligentes.[6] Projeções do impacto econômico global se aproximam de US$ 11 trilhões em 2025.[7]

Por conta desse tipo de estimativa, a IoT tem recebido fortes investimentos do setor privado e também surge como solução para diversos desafios de gestão pública. A partir do uso de tecnologias integradas e do processamento massivo de dados, a IoT promete soluções inovadoras para problemas como poluição, congestionamentos, criminalidade, eficiência produtiva, entre outros. Além disso, poderá trazer inúmeros benefícios aos consumidores. Um exemplo disto é a utilização de sistemas de automação residencial que permitam que um consumidor, antes mesmo de chegar à sua residência, possa enviar mensagem aos seus dispositivos para que realizem ações, tais como abrir os portões, desligar alarmes, colocar música ambiente e alterar a temperatura da casa.

Por outro lado, esses dispositivos conectados que nos acompanharão diária e constantemente irão coletar, transmitir, armazenar e compartilhar uma quantidade enorme de dados, muitos deles particulares e íntimos. Com o aumento exponencial da utilização destes dispositivos, é importante atentar para os riscos que isso pode trazer para a privacidade e segurança dos usuários.

---

[3] Dados semiestruturados são aqueles em que o esquema de representação está presente de forma explícita ou implícita, devendo ser feita uma análise do dado para que a sua estrutura possa ser identificada e extraída. Os dados não estruturados são aqueles que não possuem uma estrutura definida, normalmente caracterizados por documentos, textos, imagens, vídeos etc. Dados estruturados, por sua vez, são aqueles organizados em blocos semânticos (relações), provenientes de um mesmo grupo e possuindo as mesmas descrições, atributos, estrutura e formato.

[4] Vale dizer que nem todas as coisas conectadas são inteligentes. Quanto maior a autonomia e diversidade de habilidades, maior será sua inteligência. Para um aprofundamento no tema ler MAGRANI, 2018.

[5] FTC STAFF REPORT, 2015.

[6] BARKER, 2014.

[7] Cf. ROSE; ELDRIDGE; CHAPIN, 2015, p. 1 e 4.

Considerando esse cenário, este artigo visa esclarecer aspectos básicos sobre o fenômeno de IoT, sem a pretensão de esgotar todas as discussões sobre o assunto. Para atender a esse objetivo, analisa-se, em primeiro lugar, o potencial econômico e social da IoT em relação ao caso brasileiro. Em seguida, abordando-se o recente Plano Nacional de Internet das Coisas (Plano Nacional de IoT). Finalmente, trata-se dos aspectos negativos da IoT, a partir de reflexões críticas ao fenômeno com relação à privacidade e segurança cibernética.

Reflete-se, ainda, sobre como dados oriundos de dispositivos interconectados podem oferecer riscos a direitos constitucionais dos usuários, a exemplo da privacidade e segurança, podendo expô-los a prejuízos dos quais não têm ainda plena consciência. Por isso, é fundamental que os consumidores estejam atentos a esses riscos e sejam ainda mais cuidadosos com seus dados em um ambiente de Internet das Coisas. Além disso, é importante que as regulações pensadas para esse ambiente não crie obstáculos desnecessários para o desenvolvimento econômico e tecnológico em andamento e, ao mesmo tempo, regule com eficácia essas práticas, visando coibir abusos e protegendo os direitos constitucionais vigentes.

Benefícios econômicos, estatais e empresariais

A IoT tem sido encarada com otimismo por setores da indústria, podendo se tornar um dos seus principais componentes econômicos nas próximas décadas. A estimativa de impacto econômico global vinculado ao cenário de IoT corresponde a mais de US$ 11 trilhões em 2025.[8] Em pesquisa realizada pela consultoria Accenture, estima-se que "a participação da economia digital no PIB do Brasil saltará dos atuais 21,3% para 24,3% em 2020 e valerá cerca de US$ 446 bilhões (R$ 1,83 trilhão)".[9]

O Brasil está na posição de número 57 do índice de competitividade mundial[10] (*World Competitiveness Yearbook*), de 2016.[11] O anuário compara o desempenho de 63

8 Idem
9 WENTZEL, 2016.
10 Trata-se do principal relatório anual sobre a competitividade dos países publicado pelo *International Institute for Management Development* desde 1989.
11 IMD, 2016.

países, baseando-se em mais de 340 critérios que medem diferentes aspectos da competitividade. Tanto no aspecto de competitividade, quanto no quesito de inovação, seja por via pública ou privada, o Brasil deixa a desejar. Fato é que a economia do país possui potencial para se desenvolver, caso tenha as estruturas e os incentivos necessários. É justamente nesse contexto que o cenário de hiperconectividade e Internet das Coisas (IoT) deve ser considerado, já que pode contribuir para aumentar a produtividade, criar novos mercados e incentivar a inovação.

A comunidade empresarial brasileira, inclusive, reconhece o potencial da IoT. "Em recente pesquisa da Accenture com mais de 1.400 executivos de 32 países, os entrevistados brasileiros revelaram estar muito conscientes das oportunidades que a IoT pode oferecer"[12] e destacaram três principais benefícios esperados: o aumento da produtividade dos funcionários, o corte de custos e a otimização na utilização de seus bens. Também salientam a melhor experiência dos consumidores como um dos benefícios esperados.[13]

Identificou-se grande potencial para a introdução de soluções/produtos associados às tecnologias incorporadas pela IoT no desenvolvimento nacional do setor de serviços, que representa parcela importante na economia brasileira.[14] Este pode e deve ser desenvolvido a partir da IoT, com desdobramentos importantes para o restante da economia.

Além disso, deve-se atentar também para questões jurídicas e técnicas referentes a: (i) interoperabilidade entre as máquinas; (ii) ética na comunicação máquina a máquina (M2M);[15] (iii) ética na utilização de dados pessoais dos usuários; (iv) reavaliação do cenário de desenvolvimento tecnológico nacional (com implicação direta no sistema nacional de registro de patentes e transferência de tecnologia); (v) diagnóstico das políticas públicas na seara tecnológica do país.

O impacto desse fenômeno vem sendo atrelado ao conceito – ainda em construção – de "quarta revolução industrial". No fim do século XVIII, a primeira revolução industrial foi marcada pela instrumentalização da água e vapor para mover máquinas na Inglaterra. A segunda, que teve início na metade do século XIX, veio com o emprego de energia elétrica na produção em massa de bens de consumo. A terceira foi iniciada em meados do século

[12] PURDY; DAVARZANI; OVANESSOFF, 2015.
[13] ACCENTURE, 2015.
[14] MOREIRA, 2016.
[15] *Machine to Machine communication*, em inglês.

passado, e diz respeito ao uso da Internet e outras tecnologias da informação e comunicação (TICs) em processos diversos do cotidiano. A chamada "quarta revolução industrial", por sua vez, teria se iniciado na virada deste século e tem se construído a partir da revolução digital. Ela se caracteriza essencialmente por uma Internet ubíqua e móvel, por sensores e dispositivos que cada vez mais se tornam mais baratos e menores e pelo desenvolvimento da inteligência artificial.[16]

A evolução da Internet das Coisas e seu uso crescente levará à criação de novos modelos de negócios, serviços e produtos que tenderão a fortalecer a relação entre produtos e serviços. Isto pode alterar substancialmente a relação entre produtor e consumidor. Nessa linha de raciocínio, "integrar os serviços ao núcleo das políticas industriais, tecnológicas, comerciais e de investimentos parece ser uma providência fundamental para elevar a competitividade industrial".[17]

No âmbito do poder público, os benefícios da IoT podem oferecer maior eficiência da gestão pública. A partir do uso de tecnologias integradas e do processamento massivo de dados, soluções mais eficazes para problemas como poluição, congestionamentos, criminalidade, eficiência produtiva, entre outros, têm sido identificadas e implementadas. No Brasil, já existem exemplos de aplicações de IoT nesse contexto – e essas experiências tendem a aumentar.

Um exemplo disto ocorre no âmbito federal. Por meio de iniciativas do Ministério das Cidades e do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), planos nacionais que envolvem a IoT já estão sendo pensados e desenvolvidos. O primeiro deles foi proposto pelo Ministério das Cidades e prevê a criação de um projeto piloto de IoT no país, chamado Sistema Nacional de Identificação Automática de Veículos (SINIAV).[18] Esse programa consiste na instalação de identificadores (*tags*, em inglês) em veículos nacionais e importados, com o intuito de permitir sua identificação por radiofrequência, o que facilita a prevenção, fiscalização e repressão ao roubo e furto de veículos e de cargas.[19] Outro plano, proposto pelo MCTIC, em parceria com o BNDES, é mais ambicioso e define as medidas necessárias para que essa tecnologia seja promovida

[16] Idem.
[17] Ibidem, p. 12.
[18] TI RIO, 2015.
[19] LEITÃO, 2012.

como um modelo de desenvolvimento de setores como o automobilístico, o agropecuário e o urbanístico no país.

Diante deste contexto, a partir de 2017, o governo brasileiro deu início a uma série de iniciativas, o que inclui grupos de trabalho e consultas públicas, a fim de propor políticas e regulação específica para a IoT. A importância desse tipo de atividade está no desenvolvimento de um conjunto de normas que seja capaz de atender à inovação característica da IoT e, ao mesmo tempo, proteger direitos fundamentais dos cidadãos.[20] Em outras palavras, o Estado deve aprovar regulações que protejam os direitos individuais e criar mercados eficientes que favoreçam a inovação de caráter nacional.

O Plano Nacional de Internet das Coisas

Em dezembro de 2016, o BNDES e o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) assinaram um acordo de cooperação técnica para elaborar o Plano Nacional de Internet das Coisas no Brasil (Plano Nacional de IoT), o qual definirá as medidas a serem tomadas para que o país promova a Internet das Coisas como modelo de desenvolvimento para diversos setores. Por meio de chamada pública, o consórcio, que inclui o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CPqD) e a consultoria McKinsey, apresentou ao MCTIC uma proposta de estudo para oferecer os primeiros subsídios para um Plano Nacional de Internet das Coisas.

Em novembro de 2017, na fase preliminar de pesquisa, foi publicado um Relatório do Plano de Ação,[21] destacando iniciativas, projetos mobilizadores e uma seleção de critérios-chave para priorização de verticais e horizontais. Foram estruturadas diversas iniciativas organizadas em quatro **horizontais**: (i) capital humano; (ii) inovação e inserção internacional; (iii) infraestrutura de conectividade e interoperabilidade; e (iv) marco regulatório, segurança e privacidade. Para cada horizontal, foram definidos objetivos específicos. Já a análise de **verticais** refere-se a cidades, saúde, indústrias de base, casas,

[20] Somado a isso, o Congresso Nacional aprovou no dia 16 de maio de 2018 o Projeto de Lei de Conversão (PLV) 6/2018, decorrente da medida provisória (MP) 810/2017, que autoriza empresas de tecnologia da informação e da comunicação a investir em atividade de pesquisa, desenvolvimento e inovação como contrapartida para recebimento de isenções tributárias. O texto segue agora para sanção presidencial.
[21] BNDES, 2017a.

lojas, fábricas, escritórios e ambientes administrativos, logística, veículos e área rural,[22] de modo que as quatro áreas definidas como prioritárias para a atuação do Brasil através da IoT foram: (i) cidades inteligentes; (ii) saúde; (iii) área rural e; (iv) indústria.

Dando prosseguimento ao estudo, foi publicado o Capítulo Regulatório do Relatório do Plano de Ação.[23] O documento abarca as diversas áreas que podem ser beneficiadas pela IoT, bem como as possibilidades técnicas para atingir objetivos de implementação.[24] Segundo Thiago Lopes, secretário de política de informática do MCTIC, o Plano Nacional de IoT foca em quatro vertentes prioritárias de investimento, sendo elas: saúde, cidades inteligentes, agricultura e manufatura avançada.[25]

Quanto à privacidade e *proteção de dados*, o plano aponta para a necessidade de criação de uma Autoridade de Proteção de Dados Pessoais – questão largamente debatida ao longo do desenvolvimento da Lei de Proteção de Dados (13.709/2018), mas que permaneceu indefinida no texto final. Tanto a aprovação de uma lei específica, quanto a criação de autoridade de supervisão servem para mitigar as principais lacunas jurídicas existentes no contexto da proteção à privacidade no Brasil, além prevenir, de forma mais eficaz, os abusos na coleta e tratamento de dados pessoais dos usuários de Internet e nos sistemas de Internet das Coisas.

No tocante ao debate sobre cidades inteligentes, a prestação de serviços públicos importará, cada vez mais, na forma como dados pessoais são coletados, armazenados e compartilhados. Em razão disso, é crucial a adoção de medidas capazes de inibir a utilização ilegal de dados e a vigilância indevida do indivíduo por parte do Estado e de entidades privadas.

De fato, o regime de proteção à privacidade no Brasil apresenta significativas lacunas relacionadas à inexistência de uma instituição que centralize o tratamento da temática. No Plano Nacional de IoT, recomenda-se a criação de uma única instância reguladora que seja centralizada e possibilite a participação de atores relevantes, como corpo técnico especializado (nos campos tecnológico, jurídico, econômico, mercadológico, entre outros), e dotada de independência financeira e decisória.

---

[22] BNDES, 2017b.
[23] Idem.
[24] Idem.
[25] Idem.

O Plano Nacional de IoT é parte importante da Estratégia Brasileira para a Transformação Digital, definida em decreto promulgado pelo presidente Michel Temer, em março de 2018, e que contém diretrizes gerais de inovação, inclusive para ministérios do governo federal. Em maio do mesmo ano, chegou à Casa Civil da Presidência da República a minuta do Decreto do Plano Nacional de IoT, voltado para sua institucionalização. A proposta ratifica a ideia de que o marco regulatório evitará a imposição de barreiras aos novos modelos de negócio, e garantirá o direito à anonimização, ou seja, a dados que não contenham elementos de identificação. A principal preocupação da sociedade civil, porém, é a privacidade e segurança dos dados pessoais coletados e tratados a partir de tecnologias de IoT. Os próximos passos necessariamente envolvem os desdobramentos do decreto sobre a política nacional de Internet das Coisas.

Segundo o diretor de Inovação, Ciência, Tecnologia e Inovação do MCTIC, José Gontijo,[26] a definição que consta no decreto é que a Internet das Coisas é a "infraestrutura global que possibilita a prestação de serviços de valor adicionado pela conexão (física ou virtual) de 'coisas' com 'dispositivos' baseados nas tecnologias da informação e comunicação existentes e nas suas evoluções com interoperabilidade". Mas ao estabelecer que IoT é uma infraestrutura, o governo descarta sua categorização enquanto serviço de telecomunicações, o que significa que poderá ter carga tributária mais palatável do que os atuais 45% pagos atualmente por esse tipo de serviço.[27] Para Gontijo, uma das questões mais importantes a serem definidas na regulamentação é o uso dos dados pessoais e corporativos.

Nesse sentido, a Agência Nacional de Telecomunicações (Anatel) deverá definir as regras para as aplicações de IoT – Internet das Coisas – a partir do segundo semestre de 2018, dependendo das diretrizes do decreto presidencial que define as políticas públicas para a IoT no Brasil.[28] Um dos principais desafios técnicos e regulatórios que o Brasil

[26] AQUINO, 2018.
[27] Idem.
[28] O dilema de considerar a IoT como serviço de telecomunicações ou de valor adicionado é crucial, porque esta definição terá implicações sobre o imposto que o prestador de serviço deverá pagar. No entanto, o decreto enquadra IoT como infraestrutura que possibilita a prestação de serviços de valor adicionado pela conexão física ou virtual de coisas com dispositivos baseados nas tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade. De acordo com essa definição, tal infraestrutura não se confunde com a prestação de serviços de telecomunicações. No entanto, permanecem divergências sobre a necessidade de disposição legislativa e se a neutralidade da rede, estabelecida no Marco Civil da Internet, será aplicada também para a comunicação entre coisas (M2M).

enfrentará a partir desse momento diz respeito justamente ao papel do Estado em uma realidade hiperconectada. Conforme explicitado anteriormente, já há uma compreensão do Estado sobre essa necessidade. Considerando isso, o ecossistema regulatório brasileiro precisa se ajustar rapidamente a esse cenário em transformação.

Incentivos, benefícios e desafios para empresas no contexto de IoT

No setor privado, o entusiasmo com o potencial econômico da IoT tem promovido um forte investimento nessa área. Tais tendências também são identificáveis no setor denominado de *industrial IoT* (Internet das Coisas Industriais, em português), que é voltado para soluções de infraestrutura, como cidades inteligentes, rastreamento de cargas, agricultura de precisão e gerenciamento de energia e ativos. A IBM, por exemplo, é uma das pioneiras nesse setor, e investiu por volta de três bilhões de dólares em seu negócio de IoT,[29] além de fechar parceria com a AT&T[30] para fornecer soluções IoT industriais em uma série de setores – desde a eficiência energética até serviços de saúde.[31]

Essas novas frentes de investimento decorrem das perspectivas de lucro positivo da IoT. Somente a título de exemplo, cabe ressaltar a pesquisa realizada pela Cisco, que estima que a Internet das Coisas pode adicionar cerca de 352 bilhões de dólares à economia brasileira até o final de 2022.[32] Previsões como essa denotam um potencial de inovação e investimentos que atrai tanto governos quanto empresas que estão desenvolvendo iniciativas concretas.

Em relação às áreas em que essas tecnologias são empregadas, 22% dos 640 projetos de IoT são voltados para o ambiente da indústria, um quinto para cidades inteligentes e 13% para o setor de energia e carros conectados. A região que concentra a maior aplicação desse tipo de tecnologia é a América do Norte, seguida da Europa, e, por

[29] BASSI, 2015.
[30] SLOWEY, 2017.
[31] Outras empresas, como a plataforma Watson IoT, combinam um ambiente de desenvolvimento e produção baseado em nuvem para aplicativos, *software* e serviços personalizados para indústrias específicas, além de análises cognitivas.
[32] DREHER, 2015.

fim, Ásia e Oceania. Isso ilustra uma maior adesão ao uso da tecnologia de IoT nesses setores.[33]

No entanto, o investimento realizado por essas empresas pode não ser tão vantajoso se elas pretenderem expandir seus negócios, já que os custos em relação ao pagamento de *royalties* para propriedade intelectual e desafios de interoperabilidade podem diminuir significativamente a margem de lucro.

Essas dificuldades explicam por que algumas empresas se aglomeraram em *clusters*, formando alianças e consórcios em torno de questões de IoT. Esses tipos de junções têm por objetivo potencializar os benefícios da IoT de forma a gerar uma estrutura única, segura, aberta e interoperável entre os produtos e serviços dessa tecnologia. Entre os *clusters* do setor, cabe destacar o Open Interconnect Consortium (OIC) e o AllSeen Alliance.

Nesse contexto, parcerias tomam um papel importante em promover a interoperabilidade entre dispositivos conectados de ambos os grupos, permitindo maior potencial operacional da IoT e expandindo o ecossistema de produtos conectados. Este é o caso da AllSeen Alliance, fornecedora de estrutura de IoT de código aberto, que recentemente se fundiu com a Open Connectivity Foundation[34] e vem promovendo projetos *open source*, tal como o IoTivity.[35] O projeto tem o intuito de desenvolver estruturas e serviços para o aprimoramento de conexão entre dispositivos.

No campo da pesquisa, destaca-se duas parcerias que objetivam concretizar o potencial da Internet das Coisas no Brasil. A primeira, realizada pela Huawei e pela PUC-RS,[36] se propõe a criar um novo sistema de iluminação pública, em que a tecnologia IoT determinaria o momento em que a luminária está queimada ou perto de queimar. A segunda foi a criação do projeto Inatel Smart Campus,[37] cujo objetivo é desenvolver projetos de Internet das Coisas. A expectativa é que o projeto crie uma rede de conectividade com tecnologias relacionadas à IoT que possam conversar entre si.

---

[33] Os dados foram coletados a partir da tabela IoT Analytics, disponível em: <https://iot-analytics.com/wp/wp-content/uploads/2016/08/List-of-640-IoT-projects-min.png>. Acesso em: 25 jan. 2017.
[34] ALLSEEN ALLIANCE, 2016.
[35] Essa fusão terá a liderança das empresas AB Electrolux, Arçelik AS, ARRIS International plc, CableLabs, Canon, Inc., Cisco Systems, Inc., GE Digital, Haier, Intel, LG Electronics, Microsoft, Qualcomm, Samsung Electronics e Technicolor S.A.
[36] IT FORUM, 2016.
[37] INATEL, 2016.

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

Exploraremos, no item seguinte, alguns aspectos negativos relacionados ao contexto de IoT, tecendo reflexões críticas sobre o fenômeno e sua relação com a privacidade e segurança cibernética.

Reflexões críticas sobre o fenômeno: riscos à privacidade e segurança cibernética

O aumento na produção e tratamento de dados decorrente da acelerada digitalização impactará profundamente a relação existente entre consumidores, máquinas e empresas. Desafios no âmbito da segurança de dados no contexto da IoT já vêm sendo debatidos por especialistas.[38] Até o momento, empresas não conseguiram garantir suficientemente a segurança e a privacidade dos dados com a mesma velocidade e empenho com que desenvolvem os dispositivos interconectados e sistemas que têm por base a coleta de dados pessoais.

Não há consenso entre fabricantes de produtos de IoT – ou mesmo entre desenvolvedores – sobre que tecnologias e métodos são capazes de assegurar a proteção de dados pessoais e empresariais em seus produtos. A fórmula indicada é continuar com a prática de testes de vulnerabilidade em softwares e sistemas, além de também conscientizar os usuários a manterem seus dispositivos sempre atualizados com as ferramentas de segurança acessíveis.

O desafio da segurança de dados no cenário de IoT também se refere à gestão de armazenamento de dados, servidores e redes de *data centers*, além da responsabilidade jurídica de cada empresa que opera nessa cadeia de produtos e serviços. Isso decorre do

[38] DONEDA; ALMEIDA; MONTEIRO, 2015.

crescimento dos dispositivos conectados, que aumenta o volume de dados capturados e de operadores que atuam nesta cadeia econômica.

A IoT abrange diversos setores – alguns deles considerados delicados, como saúde e meio ambiente –, o que suscita desafios de segurança frente ao grande fluxo de dados que gera. Pesquisas recentes apontam graves falhas de segurança em aparelhos interconectados. A HP Security Research detectou que 70% dos dispositivos estão propensos a ataques de *hackers*.[39] Os principais problemas encontrados incluem falhas de privacidade, autorizações insuficientes para atender ao critério de consentimento expresso e informado, falta de criptografia no transporte de dados, interfaces *web* inseguras e *softwares* de proteção inadequados. Por essas razões, é necessário acompanhamento da complexidade da segurança no tratamento de Big Data.

Problemas de segurança de maior impacto incluem, por exemplo, a ação de *hackers*, como os ataques de negação de serviço (DDoS) ocorridos em outubro de 2016 que tiraram do ar grandes sites, como Netflix, Spotify e PayPal. O alvo desta investida foi a Dyn,[40] companhia que controla boa parte dos domínios da Internet.[41] Na ocasião, ataques coordenados sobrecarregaram os sites em questão com o envio de pedidos de pacotes em volume muito maior do que o fluxo habitual, levando à instabilidade e queda dos servidores, que não conseguem responder o volume de requisições maliciosas.[42] Além disso, entre 12 e 15 de janeiro de 2017, pouco antes da posse do presidente dos Estados Unidos, Donald Trump, o uso de um código malicioso denominado *ransomware*, que torna inacessíveis as informações de um determinado equipamento,[43] impossibilitou o acesso aos dados das câmeras da polícia de Washington.[44]

O acontecimento teve grandes proporções, pois muitos dispositivos IoT – como câmeras de segurança – foram utilizados para chegar ao servidor DNS Dyn.[45] Os atacantes se aproveitaram da baixa segurança destes dispositivos para infectá-los com uma *botnet* – um computador infectado por um código malicioso que permite a execução de tarefas de

[39] HEWLETT-PACKARD, 2014.
[40] DNS *Dyn* ou dinâmico (DDNS) é um método para atualizar automaticamente um servidor de nomes no Domain Name System (DNS).
[41] LOVELACE JR.;VIELMA, 2016.
[42] PAYÃO, 2016.
[43] CERT.Br, 201-?.
[44] WILLIAMS, 2017.
[45] DNS Dyn ou dinâmico (DDNS) é um método para atualizar automaticamente um servidor de nomes no Domain Name System (DNS).

forma automatizada, geralmente sem o conhecimento do usuário. À medida que o número de dispositivos afetados aumentava, maiores eram os danos ao servidor. Após o evento, a vulnerabilidade da IoT foi apontada como a verdadeira ameaça à manutenção da Internet e reclamaram providências no sentido de proteger melhor os dispositivos.[46]

Para Scott R. Peppet, os objetos de IoT são mais suscetíveis a falhas na segurança e a invasão por *hackers* por três motivos.[47] O primeiro é de caráter técnico, já que boa parte das empresas que pretendem atuar no cenário de IoT não são especializadas no desenvolvimento de *softwares* ou *hardwares* de alto nível, mas sim de produção de bens de consumo relativamente comuns no mercado. Para o autor, isso poderia significar que os engenheiros envolvidos com o projeto desses produtos são inexperientes em relação ao desenvolvimento de sistemas de segurança de alto nível.

O segundo é que esses tipos de objetos costumam ter forma compacta, o que dificulta que tenham capacidade de processamento complexa. Alguns objetos têm tamanho tão reduzido que sua bateria não é suficiente para processar sistemas de segurança de dados complexos.

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

Além dos riscos relacionados à segurança, há ainda potenciais riscos à proteção de dados pessoais. Os autores Jan Ziegeldorf, Oscar Morchon e Klaus Wehrle identificam algumas ameaças relacionadas às diferentes fases de utilização da tecnologia, sendo essas as fases de coleta, processamento e disseminação das informações.[48]

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

---

[46] THE GUARDIAN, 2016.
[47] PEPPET, 2014.
[48] ZIEGELDORF; MORCHON; WEHRLE, 2013.

Para Scott R. Peppet, um dos principais problemas de privacidade nos produtos inseridos no cenário de IoT é a ilusão da anonimização.[49] A problemática da falsa anonimidade dos dados não é problema exclusivo da tecnologia e está presente na maior parte dos serviços e produtos que fazemos uso cotidianamente. Em relação aos riscos para a privacidade, Paul Ohm critica a crença na anonimização dos dados e argumenta que, por mais que um dado tenha sido suprimido para garantir a privacidade do usuário, é possível reidentificá-lo (ou desanonimizá-lo) por meio do cruzamento de outras informações sobre o usuário disponíveis na rede.[50]

No contexto de IoT, Peppet argumenta que, mesmo que o conjunto de dados coletados pelos sensores seja considerado esparso, a reidentificação ainda é possível.[51] Isto porque os sensores, que são a ponta de captação de dados no universo da IoT, registram uma multiplicidade de dados e correlacionam-nos com diferentes tipos de dados, o que permite identificar traços capazes de destacar determinados usuários de outros.

Outro risco é o de rastreamento, que permite identificar a localização de um indivíduo em determinado espaço e tempo. O acesso a esse tipo de conteúdo é mais comum na fase de processamento, tendo em vista que é quando as informações de localização do usuário são compiladas sem que ele tenha o controle.

Para Jan Ziegeldorf, Oscar Morchon e Klaus Wehrle, o principal receio dos estudiosos de IoT diz respeito à falta de controle dos usuários sobre esse tipo de dado, – que é comumente disponibilizado sem seu consentimento ou então utilizado e associado à outros dados em práticas abusivas envolvendo *targeting* e *profiling*.[52]

A prática de *profiling* é, nesse sentido, outro problema potencializado por tecnologias de IoT. Esta compreende a criação de dossiês de informações sobre indivíduos, com o intuito de efetuar correlações com outras informações e perfis. Esse risco à privacidade aparece na fase de disseminação, quando determinados dados são compartilhados com terceiros.

Esses problemas levaram especialistas do setor a concluir que: “sem fundações fortes, ataques e disfunções na Internet das Coisas superarão qualquer um dos seus

[49] Idem.
[50] OHM, 2010.
[51] PEPPET, 2014.
[52] ZIEGELDORF; MORCHON; WEHRLE, 2013.

benefícios".[53] Esse tipo de tecnologia apresenta um paradoxo: ao mesmo tempo em que novos recursos geram benefícios e conforto ao consumidor, podem servir para lhe gerar danos.

Por isso, Peppet argumenta que a política de dados necessita de imediata reforma.[54] Nesse sentido, a exigência de consentimento dos usuários de serviços na internet é a principal política a ser executada por parte do Estado e empresas quando se trata das informações dos consumidores desses tipos de serviços. No entanto, no cenário de IoT, a aplicação desse tipo de política encontra desafios técnicos e legais. Esse debate não é deslocado do contexto brasileiro. Pelo contrário: ecoa reflexões fundamentais para o desenvolvimento de um pensamento crítico sobre IoT e o papel do governo e empresas nesse campo.

De fato, as políticas de privacidade enfrentam dois problemas: o da ambiguidade e o da omissão. O problema da ambiguidade se deve à indefinição do enquadramento dos dados obtidos por meio de sensores como sendo "pessoais", o que altera a maneira como esses dados podem ser utilizados pela empresa e por terceiros. A omissão, por sua vez, envolve a falha em prover informação, não ficando claro para o consumidor qual é a política de dados da empresa, o que inclui questões simples, como quem tem a posse dos dados ou é responsável por sua coleta e tratamento.

O Plano Nacional de IoT chama a atenção tanto para a segurança quanto para a privacidade do usuário. Além disso, dispositivos como a Constituição Federal, o Código Civil, o Código de Defesa do Consumidor e o Marco Civil da Internet também reforçam este aspecto. No entanto, é necessário e premente que haja regulações[55] que protejam a privacidade e os dados pessoais dos usuários de modo mais minucioso e atento aos âmbitos *online* e *offline*. Deve-se atentar, no entanto, para que tal regulação não represente um entrave ao avanço tecnológico, nos quais dispositivos de IoT poderão atuar, colhendo dados e informações pessoais relevantes.

---

[53] ROMAN; NAJERA; LOPEZ, 2011.
[54] PEPPET, 2014.
[55] Na Europa, foi aprovado pelo Conselho Europeu, em abril de 2016 e com entrada em vigor a partir de 25 de maio de 2018, o Regulamento Geral de Proteção de Dados (GDPR), que tem por objetivo reforçar e unificar a proteção de dados pessoais na União Europeia (UE). Por ser um regulamento, é diretamente aplicável a todos os Estados membros da UE, ao contrário da diretiva que o antecedeu. Portanto, vincula toda e qualquer organização que ofereça bens ou serviços que coletem dados pessoais relacionados à UE. O GDPR traz previsões importantes a serem observadas, não apenas pelas entidades que coletam e tratam dados pessoais (estejam elas dentro ou fora da UE), mas também pelos usuários titulares dos dados.

Nesse contexto, deve-se superar o pensamento dicotômico entre privacidade e segurança, e entre inovação tecnológica e segurança. O pilar da segurança dos dados é um pilar fundamental para o desenvolvimento adequado da inovação e para a concretização dos direitos fundamentais. Esse pilar é positivo também para o aumento da confiança dos usuários e pode servir como um diferencial concorrencial positivo. Essa perspectiva deve ser acompanhada pela preocupação com o desenho ético das novas tecnologias.

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

Conclusão

A Internet das Coisas (IoT) se torna mais proeminente a cada dia. Desenvolvida no contexto de evolução das tecnologias digitais e considerada por muitos como um novo paradigma, ela traz oportunidades e desafios para governos, empresas e consumidores.

Os setores público e privado estão atentos aos benefícios da IoT, principalmente no uso de tecnologias integradas e no processamento massivo de dados. As estimativas recaem sobre a geração de soluções mais eficazes para problemas ligados à gestão pública, eficiência produtiva, entre outros. Já existem diversos exemplos de aplicações de IoT pelo país, e essas experiências tendem a aumentar.

A ideia de dispositivos inteligentes interconectados e que permitem uma interação eficiente entre máquinas e humanos, auxiliando estes em suas tarefas diárias, pode parecer um cenário exclusivamente benéfico. Além disso, se consideradas individualmente, as informações geradas pelos dispositivos e plataformas *online* podem parecer irrelevantes e até inofensivas.

No entanto, os dados oriundos desses diversos dispositivos interconectados, gerados espontânea e deliberadamente pelos usuários, podem oferecer riscos a direitos constitucionais dos usuários, como privacidade e segurança, podendo expô-los a prejuízos dos quais não têm ainda plena consciência. Portanto, é fundamental que os consumidores

também estejam atentos a esses riscos e sejam ainda mais cuidadosos com seus dados em um ambiente de Internet das Coisas.

A maneira como nos relacionamos com máquinas tende a ser cada vez mais intensa. Neste contexto de Internet das Coisas, a governança e a segurança dos dados pessoais e empresariais serão fundamentais. Benefícios e riscos deverão ser sopesados de forma cautelosa por empresas e consumidores. O direito deve estar atento ao seu papel nesse contexto para, de um lado, não obstaculizar demasiadamente o desenvolvimento econômico e tecnológico em andamento, e, por outro lado, regular com eficácia essas práticas, visando coibir abusos e protegendo os direitos constitucionais vigentes.

Referências bibliográficas

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

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

AQUINO, M. Minuta de decreto está pronta e IoT não será serviço de telecom. 2018. Disponível em: <http://www.telesintese.com.br/minuta-de-decreto-esta-pronta-e-iot-nao-sera-servico-de-telecom/>. Acesso em: 10 jul. 2017.

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

BASSI, S. IBM transforma Internet das coisas em investimento estratégico bilionário. *Computer World*, 28 ago. 2015. Disponível em: <http://computerworld.com.br/ibm-transforma-Internet-das-coisas-em-investimento-estrategico-bilionario>. Acesso em: 28 abr. 2017.

BNDES. *Internet das coisas*: Um plano de ação para o Brasil. Banco Nacional do Desenvolvimento. 2017a. 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>. Acesso em: 5 mai. 2018.

BNDES. *Produto 8*: Relatório do Plano de Ação – Iniciativas e Projetos Mobilizadores. Banco Nacional do Desenvolvimento. 2017b. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-plano-de-acao-produto-8-alterado.pdf?MOD=AJPERES&CVID=m0jDUok>. Acesso em: 5 mai. 2018.

BNDES. *Plano de Ação. Relatório. Banco Nacional do Desenvolvimento*. 2017. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/f9582d36-4355-4638-b931-e2e53af5e456/8B-relatorio-final-plano-de-acao-produto-ambiente-regulatorio.pdf?MOD=AJPERES&CVID=m5WL-KC>. Acesso em: 8 mai. 2018.

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

DONEDA, D., ALMEIDA, V.; MONTEIRO, M. Governance challenges for the Internet of Things. *IEE Computer Society*, v. 19, n. 4, p. 56-59, 2015.

DREHER, F. IoT pode agregar US$ 352 bilhões à economia brasileira até 2022. *Computer World*, 9 jun. 2015. Disponível em: <http://computerworld.com.br/iot-pode-agregar-us-352-bilhoes-economia-brasileira-ate-2022>. Acesso em: 25 jan. 2017.

FTC STAFF REPORT. *Internet of things*: privacy & security in a connected world. [S.l.]: [s.n.], 2015. Disponível em: <www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-Internet-things-privacy/150127iotrpt.pdf>. Acesso em: 28 mar. 2017.

HEWLETT-PACKARD COMPANY. *Internet of Things Research Study Report*, jul. 2014. Disponível em: <http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VZRsHflVhHw>. Acesso em: 8 fev. 2017.

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

INATEL. Um Campus Aberto à pesquisa e testes para mercado de IoT. *Inatel*, set. 2016. Disponível em: <www.inatel.br/imprensa/noticias/pesquisa-e-inovacao/2938-um-campus-aberto-a-pesquisa-e-testes-para-mercado-de-iot>. Acesso em: 25 jan. 2017.

IT FORUM. Huawei e PUCRS abrem centro de inovação com foco em cidades inteligentes e IoT. *IT Forum*, 24 abr. 2016. Disponível em: <http://itforum365.com.br/noticias/detalhe/119237/huawei-e-pucrs-abrem-centro-de-inovacao-com-foco-em-cidades-inteligentes-e-iot>. Acesso em: 25 jan. 2017.

LANE, J.; STODEN, V.; BENDER, S.; NISSENBAUM, H. *Privacy, big data and the public good*: frameworks for engagement. Nova York: Cambridge University Press, 2014.

LEITÃO, T. Sistema de identificação automática de veículos entrará em funcionamento em janeiro. *EBC*, 3 out. 2012. Disponível em: <www.ebc.com.br/2012/10/sistema-de-identificacao-automatica-de-veiculos-entrara-em-funcionamento-em-janeiro>. Acesso em: 4 mai. 2017.

LOVELACE JR., B.; VIELMA, A. J. Friday's third cyberattack on Dyn 'has been resolved', company says. *CNBC*, 21 out. 2016. Disponível em: <http://www.cnbc.com/2016/10/21/major-websites-across-east-coast-knocked-out-in-apparent-ddos-attack.html>. Acesso em: 8 fev. 2017.

MAGRANI, E. *A internet das coisas*: privacidade e ética na era da hiperconectidade. Tese (Doutorado em Direito), Pontifícia Universidade Católica do Rio de Janeiro, 2018.

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

OHM, P. Broken Promises of Privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, v. 57, p. 1701-1777, 2010.

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

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

PURDY, M.; DAVARZANI, L.; OVANESSOFF, A. Como a Internet das coisas pode levar à próxima onda de crescimento no Brasil. *Harvard Business Review Brasil*, nov. 2015.

Disponível em: <http://hbrbr.uol.com.br/como-a-Internet-das-coisas-pode-levar-a-proxima-onda-de-crescimento-no-brasil/>. Acesso em: 28 jun. 2016.

ROMAN, R.; NAJERA, P.; LOPEZ, J. Securing the Internet of Things. *IEEE Computer*, v. 44, p. 51 -58, 2011.

ROSE, K.; ELDRIDGE, S.; CHAPIN, L. The Internet of things: an overview. Understanding the issues and challenges of a more connected world. *The Internet Society*, out. 2015. Disponível em: <www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf>. Acesso em: 30 mar. 2017.

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

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

TI RIO. GOVERNO ADIA, mais uma vez, megapiloto de Internet das coisas no país. *TI RIO*, jun. 2015. Disponível em: <www.tirio.org.br/info/35868/governo-adia-mais-uma-vez-megapiloto-de-Internet-das-coisas-no-pais>. Acesso em: 25 jan. 2017.

WENTZEL, M. Quarta revolução industrial: como o Brasil pode se preparar para a economia do futuro. *BBC Brasil*, 22 jan. 2016 Disponível em: <www.bbc.com/portuguese/noticias/2016/01/160122_quarta_revolucao_industrial_mw_ab >. Acesso em: 28 mar. 2017.

WILLIAMS, C. Hackers hit D.C. police closed-circuit camera network, city officials disclose. *The Washington Post*, 27 jan. 2017 Disponível em:

<https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.3dc5da77508f> Acesso em: 30 mar. 2017

ZIEGELDORF J.; MORCHON, O.; WEHRLE K. Privacy in the Internet of Things: Threats and Challenges. *Revista Security and Communication Networks*, v. 7, n. 12, p. 2728- 2742, 2013.