INSTITUTO IGARAPÉ
a think and do tank

ARTIGO
ESTRATÉGICO
37
NOVEMBRO 2018

A Internet das Coisas no Brasil:

Estado da arte e reflexões críticas ao fenômeno

Eduardo Magrani

Sumário

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

Por Eduardo Magrani

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. A Internet das Coisas 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 deste cenário de hiperconectividade, que acompanha a construção de um Plano Nacional de Internet das Coisas no Brasil.

Introdução

A tecnologia está mudando rapidamente a maneira como interagimos com o mundo a 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 (IoT, do inglês Internet of Things),[1] e não há consenso sobre um que seja capaz de abarcar a complexidade sociotécnica do fenômeno. O que as definições de IoT têm em comum é que apontam para 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 que cria um ecossistema de computação onipresente, com o objetivo de facilitar e trazer soluções para desafios cotidianos, como soluções na área de saúde, mobilidade urbana, e saneamento.

1 A expressão Internet das Coisas se refere a objetos que contêm sensores conectados que captam e tratam informações. Tendo em vista a necessidade de despertarmos uma consciência (crítica) no público não especializado no tema, entende-se que, por ser, de fato, menos técnica, essa nomenclatura atende melhor essa necessidade do que a abordagem pautada 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 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 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]

Algumas pesquisas estimam que, em 2020, a quantidade de objetos interconectados passará dos 25 bilhões, podendo chegar a 50 bilhões de dispositivos inteligentes

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 diversos problemas como poluição, congestionamentos, criminalidade, eficiência produtiva, entre outros. Além disso, poderá trazer inúmeros benefícios aos consumidores. Um exemplo é a utilização de sistemas de automação residencial que permita que um consumidor, antes mesmo de chegar a sua residência, possa enviar mensagem aos seus dispositivos para que realizem ações como abrir portões, desligar alarmes e alterar a temperatura da casa.

Por outro lado, esses dispositivos conectados nos acompanharão diariamente e 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 à privacidade e à segurança dos usuários.

Considerando esse cenário, este artigo visa esclarecer aspectos básicos sobre o fenômeno de IoT. Para isso, analisa, em primeiro lugar, o **potencial econômico e social da IoT no Brasil**. Em seguida, aborda o recente Plano Nacional de Internet das Coisas. Finalmente, trata dos aspectos negativos da IoT, a partir de reflexões críticas ao fenômeno com relação à privacidade e segurança cibernética. Reflete, 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 há 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 criem 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.

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, estruturas e formatos.

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

5 FTC STAFF REPORT (2015).

6 BARKER (2014); ROSE; ELDRIDGE; CHAPIN (2015, p.1, 4).

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 até 2025.[7] Pesquisa realizada pela consultoria Accenture estima 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)".[8]

A estimativa de impacto econômico global vinculado ao cenário de IoT corresponde a mais de

11 trilhões de dolares até 2025

O Brasil está na posição de número 57 do índice de competitividade mundial[9] (World Competitiveness Yearbook) de 2016.[10] O anuário compara o desempenho de 63 países com base 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 **contribui para aumentar a produtividade**, criar novos mercados e incentivar a inovação.

A comunidade empresarial, inclusive, reconhece o potencial da IoT. Executivos brasileiros entrevistados pela já citada pesquisa da Accenture destacaram três principais benefícios esperados: o aumento da produtividade dos funcionários, o corte de custos e a otimização na utilização de seus bens. Também salientaram a melhor experiência dos consumidores como um dos benefícios esperados.[11] 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.[12] Esse setor pode e deve ser desenvolvido a partir da IoT, com desdobramentos importantes para o restante da economia.

Para além das expectativas do mercado, deve-se atentar também para **questões jurídicas e técnicas** referentes a: i) interoperabilidade entre as máquinas; ii) ética na comunicação máquina a máquina (M2M);[13] 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.

7 Idem, Ibidem.

8 WENTZEL (2016).

9 Trata-se do principal relatório anual sobre a competitividade dos países publicado pelo International Institute for Management Development desde 1989.

10 IMD (2016).

11 ACCENTURE (2015).

12 MOREIRA (2016).

13 Machine to Machine communication, em inglês.

O impacto desse fenômeno vem sendo atrelado à ideia – 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 teve início na metade do século XIX, com o emprego de energia elétrica na produção em massa de bens de consumo. Já a terceira foi iniciada em meados do século 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, a partir da revolução digital. Ela se caracteriza essencialmente por uma Internet ubíqua e móvel, por sensores e dispositivos - que se tornam cada vez mais baratos e menores - e pelo desenvolvimento da inteligência artificial.[14]

A evolução da Internet das Coisas e seu uso crescente levará à criação de novos modelos de negócios, serviços e produtos que podem 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"[15]

Na esfera do poder público, os benefícios da IoT podem oferecer maior eficiência à 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 de Ciências, Tecnologias, Inovações e Comunicações (MCTIC), planos nacionais que envolvem a IoT já estão sendo pensados e desenvolvidos. O primeiro deles, proposto pelo Ministério das Cidades, prevê a criação de um projeto-piloto de IoT no país, chamado Sistema Nacional de Identificação Automática de Veículos (SINIAV).[16] 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.[17] Outro plano, proposto pelo MCTIC, em parceria com o BNDES, é mais ambicioso: define as medidas necessárias para que essa tecnologia seja promovida como um modelo de desenvolvimento de setores como o automobilístico, o agropecuário e o urbanístico no país.

Diante deste contexto, em 2017, o governo brasileiro deu início a uma série de iniciativas, como 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 e, ao mesmo tempo, proteger direitos fundamentais dos cidadãos**.[18] Em outras palavras, o Estado deve aprovar regulações que protejam os direitos individuais e criar mercados eficientes que favoreçam a inovação de caráter nacional.

14 MOREIRA (2016).

15 Idem, Ibid., p. 12.

16 TI RIO (2015).

17 LEITÃO (2012).

18 Somado a isso, o Congresso Nacional aprovou em 16/05/2018 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 o recebimento de isenções tributárias. O texto segue agora para sanção presidencial.

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 (Plano Nacional de IoT), que 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.

Em novembro de 2017, na fase preliminar de pesquisa, foi publicado o Relatório do Plano de Ação,[19] que destaca iniciativas, projetos mobilizadores e uma seleção de critérios-chave para priorização de verticais e horizontais.[20] 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 se refere a cidades, saúde, indústrias de base, casas, lojas, fábricas, escritórios e ambientes administrativos, logística, veículos e área rural,[21] 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.

Quanto à **privacidade**, o plano aponta para a necessidade de criação de uma Autoridade de Proteção de Dados Pessoais — questão que, embora largamente debatida ao longo do processo de elaboração da Lei de Proteção de Dados (13.709/2018), 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 de 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**, o plano aponta que a prestação de serviços públicos impactará, cada vez mais, a 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. O Plano Nacional de IoT recomenda 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.

O Plano é parte importante da Estratégia Brasileira para a Transformação Digital, definida em decreto promulgado pelo presidente Michel Temer em março de 2018, contendo 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, voltada 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 com a

19 BNDES (2017a).

20 O plano denomina de verticais os ambientes mapeados (cidades, saúde, rural e indústria); e de horizontais os temas transversais a esses ambientes.

21 BNDES (2017b).

privacidade e a 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.

Um dos principais desafios técnicos e regulatórios que o Brasil enfrentará a partir desse momento diz respeito justamente ao papel do Estado em uma realidade hiperconectada

A definição de Internet das Coisas que consta no decreto é: "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".[22] No entanto, ao estabelecer que IoT é uma infraestrutura, o governo descarta sua categorização enquanto serviço de telecomunicações, o que abre a possibilidade para uma carga tributária mais palatável do que os atuais 45% pagos atualmente por esse tipo de serviço.[23] Entretanto, 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 a partir do segundo semestre de 2018, dependendo das diretrizes do decreto presidencial.[24]

Um dos principais desafios técnicos e regulatórios que o Brasil enfrentará a partir desse momento diz respeito justamente ao papel do Estado em uma realidade hiperconectada. O Plano Nacional de IoT mostra que existe uma compreensão por parte do Estado brasileiro sobre a importância dos desafios que essa realidade apresenta. Mas é necessário, ainda, que o ecossistema regulatório brasileiro se ajuste 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 na área. Tais tendências também são identificáveis no setor denominado de *industrial IoT* (**Internet das Coisas industriais**, em português), voltado para soluções de infraestrutura, como cidades inteligentes, rastreamento de cargas, agricultura de precisão e gerenciamento de energia e ativos. A IBM é uma das pioneiras, tendo investido por volta de 3 bilhões de dólares em seu negócio de IoT,[25] além de fechar parceria com a AT&T[26] para fornecer soluções IoT industriais em vários setores – de eficiência energética a serviços de saúde.[27]

22 AQUINO (2018).

23 Idem, Ibidem.

24 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. O decreto enquadra a 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, ainda há divergências sobre a necessidade de disposição legislativa, e sobre a aplicação ou não, também para a comunicação entre coisas (M2M), da neutralidade da rede, estabelecida no Marco Civil da Internet.

25 BASSI (2015).

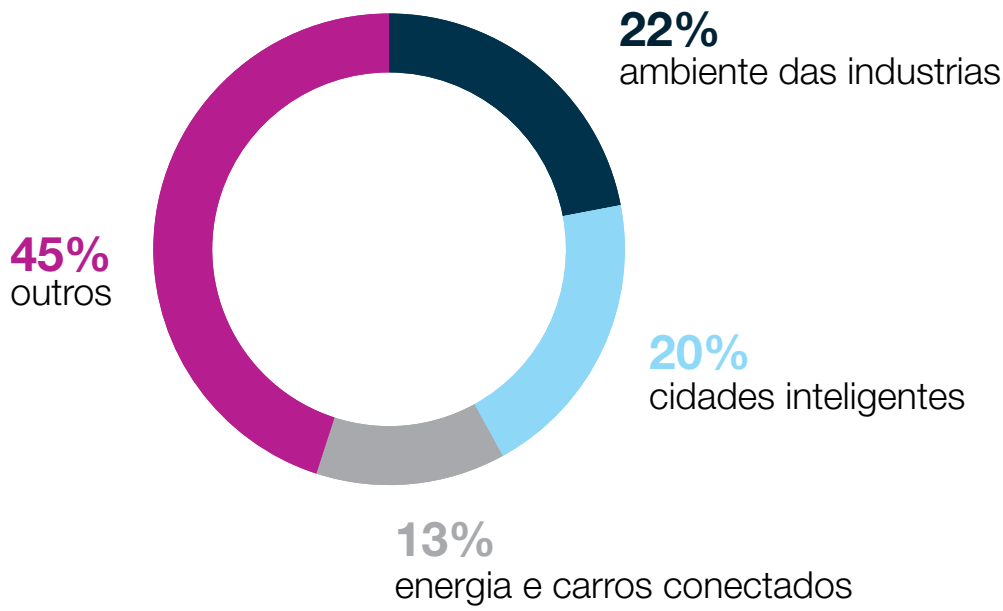
26 SLOWEY (2017).

27 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.

Essas novas frentes de investimento decorrem de perspectivas de lucro que a IoT pode gerar. 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.[28] Previsões como esta denotam um potencial de inovação e investimentos que atrai tanto governos quanto empresas que 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 fim, de Ásia e Oceania. Isso ilustra uma maior adesão ao uso da tecnologia de IoT nesses setores.[29]

Figura 1. Áreas onde são empregadas a IoT - 640 projetos



No entanto, o investimento realizado por essas empresas pode não ser tão vantajoso se elas pretendem expandir seus negócios, já que os custos em relação ao pagamento de royalties para propriedade intelectual e os desafios de interoperabilidade podem diminuir significativamente a margem de lucro. Essas dificuldades explicam por que algumas empresas formarem ***clusters***, criando 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. Como exemplos, cabe destacar o Open Interconnect Consortium (OIC) e o AllSeen Alliance.[30]

No campo da **pesquisa**, destacam-se duas parcerias que objetivam concretizar o potencial da Internet das Coisas no Brasil. A primeira, realizada pela Huawei e pela PUC-RS,[31] se propõe a criar um novo sistema de iluminação pública em que a tecnologia IoT determinaria o momento em que a luminária

28 DREHER (2015).

29 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.

30 ALLSEEN ALLIANCE (2016).

31 IT FORUM (2016).

está queimada ou perto de queimar. A segunda é a criação do projeto Inatel Smart Campus,[32] cujo objetivo é criar uma estrutura que facilite o desenvolvimento de projetos de Internet das Coisas, estimulando a pesquisa, testes de validação de conceito e tecnologias de IoT.

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 o mercado para a tecnologia IoT ainda é emergente, e deve ser devidamente regulamentado e promovido por ações político-econômicas capazes de **ampliar o crescimento econômico e o desenvolvimento nacional**.

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

O aumento na produção e tratamento de dados decorrente da acelerada digitalização impactará profundamente a **relação entre consumidores, máquinas e empresas**. Desafios no âmbito da segurança de dados no contexto da IoT já vêm sendo debatidos por especialistas.[33] 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 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 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 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**.[34] 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*.

32 INATEL (2016).

33 DONEDA; ALMEIDA; MONTEIRO (2015).

34 HEWLETT-PACKARD (2014).

Problemas de segurança de maior impacto incluem 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 dessa investida foi a Dyn,[35] companhia que controla boa parte dos domínios da Internet.[36] Na ocasião, ataques coordenados sobrecarregaram os sites em questão com pedidos de pacotes em volume muito maior do que o fluxo habitual, levando à instabilidade e à queda dos servidores, que não conseguiram responder ao volume de requisições maliciosas.[37]

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 ***ransomware***, que torna inacessíveis as informações de um determinado equipamento,[38] impossibilitou o acesso aos dados das câmeras da Polícia de Washington.[39] O acontecimento teve grandes proporções, pois muitos dispositivos IoT – como câmeras de segurança – foram utilizados para chegar ao servidor DNS Dyn. Os atacantes se aproveitaram da baixa segurança desses dispositivos para infectá-los com uma ***botnet***, um código malicioso que permite a execução de tarefas de forma automatizada 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, suscitando demandas por providências no sentido de proteger melhor os dispositivos.[40]

Scott R. Peppet aponta **três motivos** para os objetos de IoT serem mais suscetíveis a falhas na segurança e a invasões por hackers.[41] O primeiro é de caráter técnico, já que boa parte das empresas que pretendem atuar no cenário de IoT não é especializada no desenvolvimento de software 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: esse tipo de objeto costuma ter forma compacta, o que dificulta que tenham capacidade de processamento complexa. Por último, 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: coleta, processamento e disseminação das informações.[42] O principal risco é o da **identificação**, isto é, a 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 estariam mais sujeitas a esse risco devido às possibilidades de identificação facial ou por meio das digitais do indivíduo.

Para Peppet, um dos principais problemas de privacidade nos produtos inseridos no cenário de IoT é a **ilusão da anonimização**.[43] A problemática da falsa anonimidade dos dados não é problema exclusivo da tecnologia; está presente na maior parte dos serviços e produtos que usamos cotidianamente. Em relação aos riscos para a privacidade, Paul Ohm critica a crença na anonimização dos dados e

35 DNS Dyn ou dinâmico (DDNS) é um método para atualizar automaticamente um servidor de nomes no Domain Name System (DNS).

36 LOVELACE JR.;VIELMA (2016).

37 PAYÃO (2016).

38 CERT.br (s/d).

39 WILLIAMS (2017).

40 THE GUARDIAN (2016).

41 PEPPET (2014).

42 ZIEGELDORF; MORCHON; WEHRLE (2013).

43 Peppet (2014).

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 disponíveis na rede.[44]

Peppet argumenta ainda que, no contexto de IoT, mesmo que o conjunto de dados coletados pelos sensores seja considerado esparso, a reidentificação ainda é possível.[45] Isto porque os sensores, que são a ponta de captação de dados no universo da IoT, registram uma multiplicidade de dados e os correlacionam com diferentes tipos de dados, permitindo a identificação de 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 é a falta de controle dos usuários sobre esse tipo de dado, comumente disponibilizado sem seu consentimento ou utilizado e associado a outros dados em práticas abusivas como *targeting* e *profiling*.[46]

O ***profiling***, que compreende a criação de dossiês de informações sobre indivíduos com o intuito de efetuar correlações com outras informações e perfis, é um problema potencializado por tecnologias de IoT. 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 benefícios".[47] 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.[48] Nesse sentido, a exigência de **consentimento dos usuários** de serviços na Internet é a principal política a ser executada por parte do Estado e de empresas no tratamento de informações dos consumidores. 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 "pessoais", o que altera a maneira como podem ser utilizados pela empresa e por terceiros. A **omissão**, por sua vez, envolve a falha em prover informação para o consumidor sobre a política de dados da empresa, incluindo questões bastante 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

44 OHM (2010).

45 PEPPET (2014).

46 ZIEGELDORF; MORCHON; WEHRLE (2013).

47 ROMAN; NAJERA; LOPEZ (2011).

48 PEPPET (2014).

premente que haja regulações[49] que protejam a privacidade e os dados pessoais dos usuários de modo mais minucioso e atento aos âmbitos online e offline. Ao mesmo tempo, essa regulação não pode representar um entrave ao avanço tecnológico, que também pode ser potencializado pela coleta de dados pessoais relevantes por dispositivos de IoT.

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 fundamental para o desenvolvimento adequado da inovação e para a concretização dos direitos fundamentais. Ele 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 se torna mais presente a cada dia no Brasil. Desenvolvida no contexto de evolução das tecnologias digitais, 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 o número de experiências tende a aumentar.

A ideia de dispositivos inteligentes interconectados que permitem que máquinas auxiliem humanos em suas tarefas diárias pode parecer exclusivamente positiva. De fato, se consideradas individualmente, as informações geradas pelos dispositivos e plataformas online podem parecer irrelevantes e até inofensivas. No entanto, os dados oriundos de dispositivos interconectados, gerados espontânea e deliberadamente pelos usuários, também podem oferecer riscos a direitos constitucionais dos usuários, como privacidade e segurança, expondo-os a prejuízos dos quais não têm ainda plena consciência. Portanto, 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.

A maneira como nos relacionamos com máquinas tende a ser cada vez mais intensa. Nesse contexto de IoT, 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.

49 O Conselho Europeu aprovou, em abril de 2016, o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês), que entrou em vigor em 25 de maio de 2018, com o 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, 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.

Referências

ACCENTURE (2015). From productivity to outcomes: using the Internet of Things to drive future business strategies. 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 (2016). Allseen Alliance merges with open connectivity foundation to accelerate the Internet of Things. Disponível em: https://allseenalliance.org/allseen-alliance-merges-open-connectivity-foundation-accelerate-Internet-things. Acesso em: 25 jan. 2017.

AQUINO, M. (2018). "Minuta de decreto está pronta e IoT não será serviço de Telecom". Telesíntese. 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. (2014). 25 billion connected devices by 2020 to build the Internet of Things. ZDNet. 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. (2015). "IBM transforma Internet das Coisas em investimento estratégico bilionário". Computer World. Disponível em: http://computerworld.com.br/ibm-transforma-Internet-das-coisas-em-investimento-estrategico-bilionario. Acesso em: 28 abr. 2017.

BNDES (2017). Internet das Coisas: um plano de ação para o Brasil. 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 (2017). Relatório do Plano de Ação – iniciativas e projetos mobilizadores. 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 (2017). Plano de Ação. 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. (s/d). Cartilha de segurança para Internet. Disponível em: http://cartilha.cert.br/ransomware/. Acesso em: 30 mar. 2017.

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

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

FTC STAFF REPORT (2015). Internet of Things: privacy & security in a connected world. 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 (2014). Internet of Things research study report. 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 (2016). "The 2016 IMD world: competitiveness scoreboard". IMD. Disponível em: https://statistiques.public.lu/en/news/economy-finance/competitivity/2016/05/20160531/index.html. Acesso em: 28 jun. 2016.

INATEL (2016). Um campus aberto à pesquisa e testes para mercado de IoT. 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 (2016). "Huawei e PUCRS abrem centro de inovação com foco em cidades inteligentes e IoT". ITF365. 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. (2014). Privacy, big data and the public good: frameworks for engagement. Nova York: Cambridge University Press.

LEITÃO, T. (2012). Sistema de identificação automática de veículos entrará em funcionamento em janeiro. EBC. 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. (2016). Friday's third cyberattack on Dyn 'has been resolved', company says. CNBC. 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. (2018). A Internet das Coisas: privacidade e ética na era da hiperconectividade. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro.

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

OHM, P. (2010). "Broken promises of privacy: responding to the surprising failure of anonymization". UCLA Law Review, vol. 57, p. 1701-1777.

PAYÃO, F. (2016). "Quebrando a Internet: estamos sofrendo o maior ataque DDoS da história". Tecmundo. 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. (2014). "Regulating the Internet of Things: first steps toward managing discrimination, privacy, security, and consent". Texas Law Review, vol. 93, n. 85, p. 85-176.

PURDY, M.; DAVARZANI, L.; OVANESSOFF, A. (2015). "Como a Internet das Coisas pode levar à próxima onda de crescimento no Brasil". Harvard Business Review Brasil. 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. (2011). “Securing the Internet of Things”. IEEE Computer, vol. 44, p. 51 -58.

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

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

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

TI RIO (2015). “Governo adia, mais uma vez, megapiloto de Internet das Coisas no país”. TI RIO. Disponível em: https://www.ti.rio/info/35868/governo-adia-mais-uma-vez-megapiloto-de-internet-das-coisas-no-pais. Acesso em: 25 jan. 2017.

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

WILLIAMS, C. (2017). “Hackers hit D.C. police closed-circuit camera network, city officials disclose”. The Washington Post. Disponível em: https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/. Acesso em: 30 mar. 2017

ZIEGELDORF J.; MORCHON, O.; WEHRLE K. (2013). “Privacy in the Internet of Things: threats and challenges”. Revista Security and Communication Networks, vol. 7, n. 12, p. 2728- 2742.

Sobre o autor

Eduardo Magrani é doutor e mestre em Direito Constitucional e Teoria do Estado pela PUC-Rio. É *Senior Fellow* na Universidade Humboldt de Berlim, no Alexander von Humboldt Institute for Internet and Society (HIIG). É coordenador do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio), professor de Direito e Tecnologia e Propriedade Intelectual na FGV, no IBMEC e na PUC-Rio. Atua como advogado nos campos de Direitos Digitais, Direito Societário e Propriedade Intelectual. É autor de diversos livros e artigos na área de tecnologia e propriedade intelectual, entre eles: “Democracia Conectada” (2014) e “Digital Rights: Latin America and the Caribbean” (2017).

Outras publicações do Instituto Igarapé

ARTIGOS ESTRATÉGICOS

ARTIGO ESTRATÉGICO 36 - La “Mano Dura”: Los costos de la represión y los beneficios de la prevención para los jóvenes en América Latina
Adriana Erthal Abdenur
(Maio 2018)

ARTIGO ESTRATÉGICO 35 - Garantindo a paz: O Brasil e o processo de paz com o ELN da Colômbia
Adriana Erthal Abdenur
(Maio 2018)

ARTIGO ESTRATÉGICO 34 - Colômbia e as FARC: Cenários pós-conflito e repercussões regionais
Guilherme Damasceno Fonseca e Christian Vianna de Azevedo
(Maio 2018)

ARTIGO ESTRATÉGICO 33 - Citizen Security in Latin America: Facts and Figures
Robert Muggah e Katherine Aguirre Tobón
(Abril 2018)

ARTIGO ESTRATÉGICO 32 - A agenda sobre mulheres, paz e segurança no contexto latinoamericano: desafios e oportunidades
Renata Avelar Giannini, Ana Paula Pellegrino, Carol Viviana Porto, Luisa Lobato, Maiara Folly e Mariana Gomes da Rocha
(Março 2018)

ARTIGO ESTRATÉGICO 31 - Implementando a agenda sobre “Mulheres, Paz e Segurança” no Brasil: uma revisão do Plano Nacional de Ação
Paula Drumond e Tamya Rebelo
(Março 2018)

ARTIGO ESTRATÉGICO 30 - Gênero, justiça e segurança no Brasil e na Colômbia: como prevenir e tratar da violência contra mulheres?
Renata Avelar Giannini, Orlinda Cláudia Rosa de Moraes e Marcelo Diaz
(Março 2018)

ARTIGO ESTRATÉGICO 29 - Migrantes invisíveis: a crise de deslocamento forçado no Brasil
Maiara Folly
(Março 2018)

ARTIGO ESTRATÉGICO 28 - Salas de Consumo de Drogas: situando o debate no Brasil
Rafael Tobias de Freitas Alloni e Luiz Guilherme Mendes de Paiva
(Outubro 2017)

ARTIGO ESTRATÉGICO 27 - Situações extraordinárias: a entrada de mulheres na linha de frente das Forças Armadas brasileiras
Renata Avelar Giannini, Maiara Folly e Mariana Fonseca Lima
(Agosto 2017)

ARTIGO ESTRATÉGICO 26 - A percepção de crianças e adolescentes sobre a segurança e a violência: a aplicação do Indice de Segurança da Criança em uma escola
Renata Avelar Giannini, Maiara Folly, Monica de Cassia Nehrebeck e Willian Vinícius Silva
(Junho 2017)

ARTIGO ESTRATÉGICO 25 - O Brasil e o Marco Civil da Internet. O Estado da Governança Digital Brasileira
Daniel Arnaudo
(Abril 2017)

ARTIGO ESTRATÉGICO 24 - Confiança em desenvolvimento: o Brasil e os projetos de impacto rápido
Eduarda Hamann, Henrique Garbino e Maiara Folly
(Abril 2017)

ARTIGO ESTRATÉGICO 23 - Controlando el territorio y construyendo seguridad y justicia en el posconflicto colombiano. Edición especial de los Diálogos por la Seguridad Ciudadana
(Dezembro 2016)

ARTIGO ESTRATÉGICO 22 - Durões contra os fracos; fracos frente aos durões: as leis de drogas e a prática da ação policial
Juan Carlos Garzón Vergara
(Outubro 2016)

ARTIGO ESTRATÉGICO 21 - Infância e Segurança: um estudo sobre a percepção da violência por crianças e adolescentes do Complexo do Muquiço, Rio de Janeiro
Renata A. Giannini, Maiara Folly, Victor Ladeira, Andressa Werneck e Renata Siqueira
(Julho 2016)

ARTIGO ESTRATÉGICO 20 - Making Cities Safer: Citizen Security Innovations from Latin America
Robert Muggah, Ilona Szabo de Carvalho, Nathalie Alvarado, Lina Marmolejo e Ruddy Wang
(Junho 2016)

ARTIGO ESTRATÉGICO 19 - Construindo Planos Nacionais de Ação eficazes: coletânea de boas práticas
Renata A. Giannini
(Março 2016)

ARTIGO ESTRATÉGICO 18 - “When Kids Call the Shots” Children’s perceptions on violence in Recife, Brazil, as per the ‘Child Security Index’
Helen Moestue, Katherine Aguirre e Renata A. Giannini
(Dezembro 2015)

ARTIGO ESTRATÉGICO 17 - Where is Latin America? Reflections on Peace, Security, Justice and Governance in the Post-2015 Sustainable Development Agenda
Renata A. Giannini
(Outubro 2015)

ARTIGO ESTRATÉGICO 16 - Políticas de Drogas no Brasil: A Mudança já Começou
Ilona Szabó de Carvalho e Ana Paula Pellegrino
(Março 2015)

ARTIGO ESTRATÉGICO 15 - Nuevos retos y nuevas concepciones de la seguridad en México
Edición especial de los Diálogos por la Seguridad Ciudadana
(Março 2015)

ARTIGO ESTRATÉGICO 14 - A 'Third Umpire' for Policing in South Africa – Applying Body Cameras in the Western Cape
David Bruce e Sean Tait
(Março 2015)

ARTIGO ESTRATÉGICO 13 - Brazil and Haiti: Reflections on 10 Years of Peacekeeping and the Future of Post-2016 Cooperation
Eduarda Passarelli Hamann (org.)
(Janeiro 2015)

ARTIGO ESTRATÉGICO 12 - Measurement Matters: Designing New Metrics for a Drug Policy that Works
Robert Muggah, Katherine Aguirre e Ilona Szabó de Carvalho
(Janeiro 2015)

ARTIGO ESTRATÉGICO 11- Desconstruindo a segurança cibernética no Brasil: ameaças e respostas
Gustavo Diniz, Robert Muggah e Misha Glenny
(Dezembro de 2014)

ARTIGO ESTRATÉGICO 10 - Expansão Digital: como as novas tecnologias podem prevenir a violência contra crianças nos países do hemisfério sul
Helen Mostue e Robert Muggah
(Novembro 2014)

ARTIGO ESTRATÉGICO 9 - Promover Gênero e Consolidar a Paz: A Experiência Brasileira
Renata A. Giannini
(Setembro 2014)

ARTIGO ESTRATÉGICO 8 - Tornando as Cidades Brasileiras mais Seguras: Edição Especial dos Diálogos de Segurança Cidadã
Michele dos Ramos, Robert Muggah, José Luiz Ratton, Clarissa Galvão, Michelle Fernandez, Claudio Beato, Andréa Maria Silveira, Melina Ingrid Risso e Robson Rodrigues.
(Julho 2014)

ARTIGO ESTRATÉGICO 7 - Changes in the Neighborhood: Reviewing Citizen Security Cooperation in Latin America
Robert Muggah e Ilona Szabó de Carvalho
(Março 2014)

ARTIGO ESTRATÉGICO 6 - Prevenindo a violência na América Latina por meio de novas tecnologias
Robert Muggah e Gustavo Diniz
(Janeiro 2014)

ARTIGO ESTRATÉGICO 5 - Protegendo as Fronteiras: o Brasil e sua estratégia "América do Sul como prioridade" contra o crime organizado transnacional
Robert Muggah e Gustavo Diniz
(Outubro 2013)

ARTIGO ESTRATÉGICO 4 - To Save Succeeding Generations: UN Security Council Reform and the Protection of Civilians
Conor Foley
(Agosto 2013)

ARTIGO ESTRATÉGICO 3 - Momento Oportuno: Revisão da Capacidade Brasileira para Desdobrar Especialistas Civis em Missões Internacionais
Eduarda Passarelli Hamann
(Janeiro 2013)

ARTIGO ESTRATÉGICO 2 - A Fine Balance: Mapping Cyber (in)security in LatinAmerica
Gustavo Diniz e Robert Muggah
(Junho 2012)

ARTIGO ESTRATÉGICO 1- Mecanismos Nacionais de Recrutamento, Preparo e Emprego de Especialistas Civis em Missões Internacionais
Eduarda Passarelli Hamann
(Maio 2012)

NOTAS ESTRATÉGICAS

NOTA ESTRATÉGICA 30 - Uma Estratégia para a Governança da Segurança Cibernética no Brasil
Louise Marie Hurel e Luisa Cruz Lobato
(Setembro 2018)

NOTA ESTRATÉGICA 29 - Will Cuba Update its Drug Policy for the Twenty First Century?
Isabella Bellezza-Smull
(Dezembro 2017)

NOTA ESTRATÉGICA 28 - Desafios e Boas práticas para Implementação da Agenda sobre Mulheres, Paz e Segurança
Renata Avelar Giannini e Maiara Folly
(Novembro 2017)

NOTA ESTRATÉGICA 27 - À Margem do Perigo: preparo de civis brasileiros para atuação em países instáveis
Eduarda Passarelli Hamann
(Junho 2017)

NOTA ESTRATÉGICA 26 - Haitian Women's Experiences of Recovery from Hurricane Matthew
Athena Kolbe, Marie Puccio, Sophonie M. Joseph, Robert Muggah e Alison Joersz
(Junho 2017)

NOTA ESTRATÉGICA 25 - The Future of United Nations Peacekeeping Operations from a Brazilian Perspective (implementing the HIPPO report)
Eduarda Hamann and Adriana Erthal Abdenur
(Março 2017)

NOTA ESTRATÉGICA 24 - Em Busca da Igualdade de Gênero: boas práticas para a implementação da agenda sobre mulheres, paz e segurança
Maiara Folly e Renata Avelar Giannini
(Março 2017)

NOTA ESTRATÉGICA 23 - Filling the accountability gap: principles and practices for implementing body cameras for law enforcement
Robert Muggah, Emile Badran, Bruno Siqueira e Justin Kosslyn
(Novembro 2016)

NOTA ESTRATÉGICA 22 - Latin American Dialogue on International Peace and Security
Reviewing the prospects for peace operations, peacebuilding and women, peace and security
(Maio 2016)

NOTA ESTRATÉGICA 21 - Assessing Haiti's Electoral Legitimacy Crisis – Results of a 2016 Survey
Athena R. Kolbe e Robert Muggah
(Fevereiro 2016)

NOTA ESTRATÉGICA 20 - Impact of Perceived Electoral Fraud on Haitian Voter's Beliefs about Democracy
Athena R. Kolbe, Nicole I. Cesnales, Marie N. Puccio e Robert Muggah
(Novembro 2015)

NOTA ESTRATÉGICA 19 - A Força de uma Trajetória: O Brasil e as operações de paz da ONU (1948-2015)
Eduarda Passarelli Hamann
(Outubro 2015)

NOTA ESTRATÉGICA 18 - Implementing UNSC Resolution 1325 in Brazil: surmounting challenges and promoting equality
Renata A. Giannini, Mariana Lima e Pérola Pereira
(Outubro 2015)

NOTA ESTRATÉGICA 17 - A Reforma do Conselho de Segurança da ONU: visão de mundo e narrativas do Brasil
Eduarda Passarelli Hamann
(Maio 2015)

NOTA ESTRATÉGICA 16 - Break Your Bones: mortality and morbidity associated with Haiti's Chikungunya epidemic
Athena R. Kolbe, Augusta Herman e Robert Muggah (Julho 2014)

NOTA ESTRATÉGICA 15 - New Technologies for Improving Old Public Security Challenges in Nairobi
Mads Frilander, Jamie Lundine, David Kutalek e Luchetu Likaka
(Junho 2014)

NOTA ESTRATÉGICA 14 - O Despertar da América Latina: uma revisão do novo debate sobre politica de drogas
Ilona Szabó de Carvalho
(Fevereiro 2014)

NOTA ESTRATÉGICA 13 - The Changing Face of Technology Use in Pacified Communities
Graham Denyer Willis, Robert Muggah, Justin Kossyln e Felipe Leusin
(Fevereiro 2014)

NOTA ESTRATÉGICA 12 - A Inserção de Civis Brasileiros no Sistema ONU: oportunidades e desafios
Renata Avelar Giannini
(Janeiro 2014)

NOTA ESTRATÉGICA 11 - A Diáspora Criminal: o alastramento transnacional do crime organizado e as medidas para conter sua expansão
Juan Carlos Garzón Vergara
(Novembro 2013)

NOTA ESTRATÉGICA 10 - Smarter Policing: tracking the influence of new information technology in Rio de Janeiro
Graham Denyer Willis, Robert Muggah, Justin Kosslyn e Felipe Leusin
(Novembro 2013)

NOTA ESTRATÉGICA 9 - Is Tourism Haiti's Magic Bullet? An Empirical Treatment of Haiti's Tourism Potential
Athena R. Kolbe, Keely Brookes and Robert Muggah (Junho 2013)

NOTA ESTRATÉGICA 8 - Violencia, Drogas y Armas ¿Otro Futuro Posible?
Ilona Szabó de Carvalho, Juan Carlos Garzón e Robert Muggah
(Julho 2013)

NOTA ESTRATÉGICA 7 - A Promoção Da Paz No Contexto Pós-2015: o papel das potências emergentes
Robert Muggah, Ivan Campbell, Eduarda Hamann, Gustavo Diniz e Marina Motta
(Fevereiro 2013)

NOTA ESTRATÉGICA 6 - After the Storm: Haiti's coming food crisis
Athena Kolbe, Marie Puccio e Robert Muggah
(Dezembro 2012)

NOTA ESTRATÉGICA 5 - Brazil's Experience in Unstable Settings
Eduarda Passarelli Hamann e Iara Costa Leite
(Novembro 2012)

NOTA ESTRATÉGICA 4 - Cooperação Técnica Brasileira
Iara Costa Leite e Eduarda Passarelli Hamann
(Setembro 2012)

NOTA ESTRATÉGICA 3 - A Experiência do Brasil em Contextos Instáveis
Eduarda Passarelli Hamann e Iara Costa Leite
(Agosto 2012)

NOTA ESTRATÉGICA 2 - The Economic Costs of Violent Crime in Urban Haiti (Aug 2011 - Jul 2012)
Athena R. Kolbe, Robert Muggah e Marie N. Puccio
(Agosto 2012)

NOTA ESTRATÉGICA 1 - Haiti's Urban Crime Wave? Results from Monthly Households Surveys (Aug 2011 - Feb 2012)
Athena R. Kolbe e Robert Muggah
(Março 2012)

INSTITUTO IGARAPÉ
a think and do tank

O Instituto Igarapé é um think and do tank independente, dedicado às agendas da segurança, da justiça e do desenvolvimento. Seu objetivo é propor soluções inovadoras a desafios sociais complexos, por meio de pesquisas, novas tecnologias, influência em políticas públicas e articulação. O Instituto atualmente trabalha com cinco macrotemas: (i) política sobre drogas nacional e global; (ii) segurança cidadã; (iii) cidades seguras; (iv) consolidação da paz; e (v) segurança cibernética. O Instituto Igarapé tem sede no Rio de Janeiro, com representação em Bogotá, Cidade do México, Lisboa e outras partes do mundo.

Instituto Igarapé
Rua Miranda Valverde, 64
Botafogo, Rio de Janeiro – RJ – Brasil - 22281-000
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

www.igarape.org.br

Direção de arte: Raphael Durão - STORM.pt

ISSN 2359-098X

INSTITUTO IGARAPÉ
a think and do tank

Rua Miranda Valverde, 64
Botafogo, Rio de Janeiro – RJ – Brasil - 22281-000
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

www.igarape.org.br