INSTITUTO IGARAPÉ
a think and do tank

NOTA
ESTRATÉGICA
31
NOVEMBRO 2018

Segurança e privacidade para a Internet das Coisas

Louise Marie Hurel e Luisa Cruz Lobato

Sumário

Segurança e privacidade para a Internet das Coisas

Resumo

A implementação de tecnologias associadas à Internet das Coisas (IoT, da sigla em inglês) é fundamental para o desenvolvimento social e econômico do país, em especial com o uso de Tecnologias da Informação e Comunicação (TICs). No entanto, a IoT também traz uma série de riscos relacionados à segurança, privacidade e proteção de dados. Ao considerar seus impactos sociais e econômicos, esta Nota Estratégica identifica e analisa os riscos de três tecnologias que sustentam este paradigma: dispositivos e sensores, sistemas de inteligência artificial e computação na nuvem. Também explora aspectos regulatórios e técnicos importantes para o desenvolvimento de tecnologias para uma IoT segura. A pesquisa foi feita a partir da análise de documentos primários, como políticas e marcos regulatórios, além de revisão bibliográfica e reuniões com especialistas de diferentes setores. Os resultados encontrados sugerem que para mitigar estes riscos é necessária a inserção de valores e princípios fundamentais, como privacidade e segurança, ainda no início da cadeia de desenvolvimento da IoT. Argumenta-se, assim, em favor da concepção de uma IoT que vise maximizar a proteção dos dados coletados e minimizar os riscos de ataques cibernéticos. Em outras palavras, uma IoT que contribua para a construção de um ecossistema sustentável para usuários, governos e negócios.

1. Introdução

A Internet das Coisas (IoT) é composta por uma rede de objetos interconectados que se comunicam entre si,[1] como, por exemplo, veículos, prédios e eletrodomésticos. O aumento do acesso à Internet e aos mecanismos de processamento de dados facilita o crescimento e expectativa de aplicação em larga escala de dispositivos de IoT.[2] Nesse contexto, novos produtos, modelos de negócio, serviços e funcionalidades técnicas visam otimizar a qualidade de vida de muitos a partir do uso de uma combinação de tecnologias, especialmente aquelas baseadas em *analytics*.[3]

Se, por um lado, a IoT promete um aumento de investimentos em tecnologias de ponta para o setor privado e maior integração de objetos interconectados em atividades rotineiras, por outro, novos desafios com relação à segurança e à privacidade de ecossistemas conectados colocam em xeque os seus benefícios. De acordo com o *Global Risks Report,* do Fórum Econômico Mundial, ataques cibernéticos são a terceira maior ameaça global - logo depois de desastres naturais.[4] Ataques e/ou vazamento de dados de dispositivos conectados, tais como a torradeira, a geladeira ou até a babá eletrônica inteligente, expõem o consumidor a um ecossistema de dispositivos e sensores que coletam dados indiscriminadamente. Atualmente, somente 1% dos dados coletados por esses objetos e sensores são, de fato, utilizados.[5] Enquanto indivíduos desconhecem *quais* tipos de dados são coletados e *como* são compartilhados, o setor privado busca maximizar o aproveitamento deles. Nesse contexto, "coisas" também se tornam vetores de ataques em larga escala, provocando disrupções na Internet, nas redes de objetos a ela associados, e em outros setores da sociedade.[6]

No Brasil, a Internet das Coisas surge gradualmente, como resultado de mudanças significativas nas formas de acesso à rede. Atualmente, o país possui mais de 20 milhões de comunicações máquina-máquina e a expectativa é que esse número alcance os 42 milhões até 2020.[7] Isso se deve, em parte, à substituição de telefones celulares por *smartphones*[8] e à concentração do acesso à Internet por meio de serviços de banda larga móvel (2G, 3G, 4G) em todas as regiões do país.[9] Em 2017, foram mais de 188,9 milhões de acessos à Internet via dispositivos móveis em comparação a 27,8 milhões de acesso por banda larga fixa.[10]

---

1 MINERVA; BIRU; ROTONDI (2015).

2 ROSE; ELDRIDGE; CHAPIN (2015).

3 Analytics se refere aos métodos estatísticos e técnicas utilizadas para extrair insights de bases de dados. Dados não são úteis se não forem interpretados ou reorganizados por meio de determinadas técnicas. Com big data analytics, torna-se possível correlacionar bases de dados, bem como processar grandes volumes de dados, e esses processos em grande escala estão associados a tecnologias mais complexas como a inteligência artificial e o aprendizado de máquina.Ver: KITCHIN (2014).

4 WEF (2018).

5 MCKINSEY (2015b); HUNG (2017).

6 A exemplo da Mirai botnet que, em 2017, se aproveitou de vulnerabilidades em dispositivos IoT para estabelecer uma rede de objetos como parte de um ataque de negação de serviço (DDoS). Ver: KOLIAS et al. (2017).

7 MCTIC (2017).

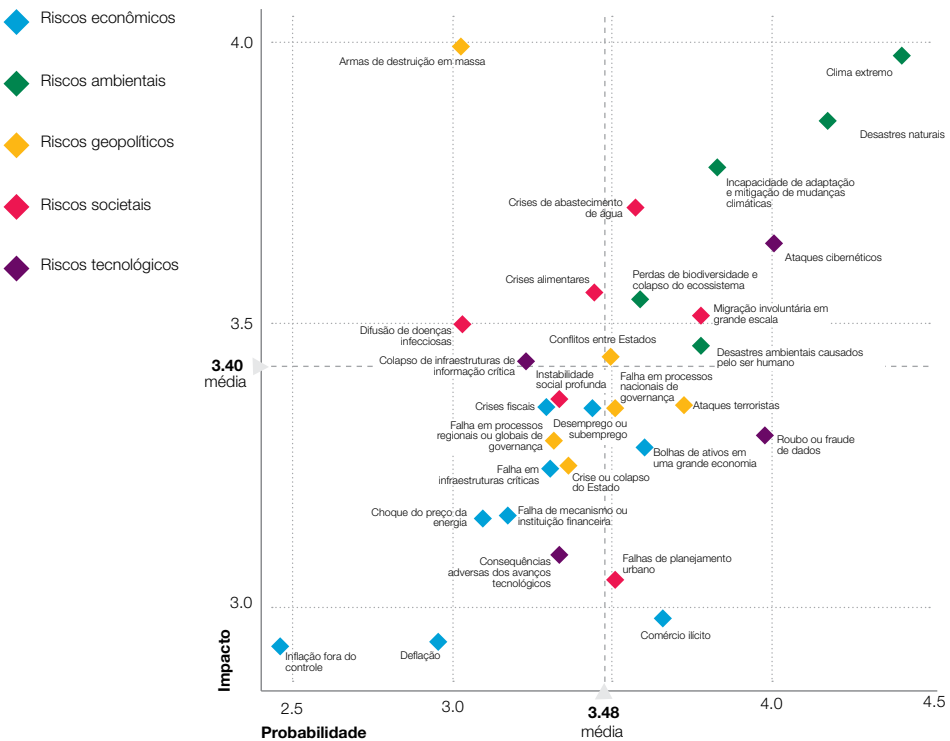
8 Idem, Ibidem.

9 CETIC (2017).

10 ANATEL (2017).

No entanto, o desenvolvimento de políticas e estratégias para a IoT, no âmbito nacional, ainda está em seus primeiros passos. Em 2018, o governo aprovou a Estratégia Brasileira para Transformação Digital e caminha para o seu Plano Nacional de Internet das Coisas (Plano Nacional de IoT).[11] Vale ressaltar que, para além da formação de uma pauta político-estratégica para o tema, faz-se necessária a garantia de um desenvolvimento sustentável (seguro e em acordo aos direitos dos indivíduos) da aplicação da IoT para setores além do consumo. A reflexão apresentada nesta nota estratégica deve ser acompanhada de contínuos esforços para o desenvolvimento uma IoT que reflita as realidades regionais no uso de dispositivos e sensores conectados. Criando, portanto, insumos para a inserção de tecnologias IoT que, de fato, beneficiem os setores mais pujantes da economia (e.x.: agricultura, agronegócio), bem como as necessidades de cidades e indivíduos no país.

Figura 1: Impacto e probabilidade de riscos globais.



Fonte: Global Risks Landscape 2018

11 MCTIC (2018).

Para fortalecer o debate sobre políticas públicas e apontar os riscos para a privacidade e segurança, torna-se igualmente fundamental compreender as tecnologias que sustentam a IoT. Neste estudo, destaca-se três grupos de tecnologias: (i) dispositivos e sensores; (ii) sistemas de inteligência artificial; e (iii) computação na nuvem. O primeiro grupo é composto por elementos de hardware, enquanto que os dois grupos restantes, por elementos de software. Argumenta-se que a incorporação dos princípios da privacidade, proteção de dados e segurança no processo de desenvolvimento dessas tecnologias é central para o avanço e consolidação da IoT em dois aspectos: tanto como um conjunto de tecnologias estratégicas que integram a elaboração de uma política de governo (Plano Nacional de IoT), como na condição de um importante ativo mercadológico, capaz de proporcionar inovações setoriais para a economia e conectividade do país. Estes valores precisam ser inseridos na concepção e design do produto, mas também constantemente reavaliados, para que permaneçam relevantes no uso do produto ou dispositivo de IoT.[12] Portanto, para que o potencial da IoT se concretize, é necessário, antes de tudo, compreender como esses princípios se aplicam à operacionalização das tecnologias supracitadas.

Os principais resultados da pesquisa foram:

- A análise do uso de sensores e dispositivos, tecnologias de computação na nuvem e inteligência artificial indicou que, de modo geral, há pouca preocupação com o desenvolvimento de tecnologias seguras (*security by design*) e garantia da privacidade do usuário (*privacy by design*) no Brasil.

- A proliferação de dispositivos e sensores que captam e processam dados sobre pessoas, ambientes e eventos traz três desafios à segurança de indivíduos e de empresas. O primeiro é a ausência de padrões técnicos compartilhados entre indústria, agências regulatórias, desenvolvedores e provedores, o que é um obstáculo à interoperabilidade entre dispositivos. O segundo é a falta de garantias de que a performance de um dispositivo não extrapole a finalidade para a qual foi programado, nem o consentimento do usuário ou empresa que o utiliza. O terceiro é que problemas de segurança da IoT também se aplicam a dispositivos desconectados, pois nem todos os objetos requerem conexão com a Internet para se comunicarem.

- A rápida integração da nuvem a dispositivos de IoT nem sempre é acompanhada pelo incremento no nível de segurança em ambos os lados. Aos problemas de segurança comumente relacionados à nuvem, somam-se aqueles específicos de dispositivos de IoT, criando um ecossistema com novas configurações de vulnerabilidades e riscos.

12 Ver: DE ROECK (2018).

- Os principais desafios para um sistema mais abrangente de governança da IoT são: a rápida difusão de sistemas ciber-físicos[13] pouco seguros e a falta de atenção aos contextos cultural, socioeconômico e regulatório no Brasil.

Os achados acima chamam a atenção para os riscos apresentados por essas novas tecnologias. Eles sugerem que, para mitigá-los, é necessário investir em sistemas seguros e menos intrusivos à privacidade dos usuários ainda no início da cadeia de desenvolvimento de produtos, serviços e soluções baseadas em IoT. Desenvolvedores e formuladores de políticas devem atentar para os riscos e valores que orientam tanto o mercado de dispositivos e soluções de IoT, quanto os que são efetivamente traduzidos em regulações, diretrizes e estratégias que possibilitam a expansão da digitalização no país, respectivamente.

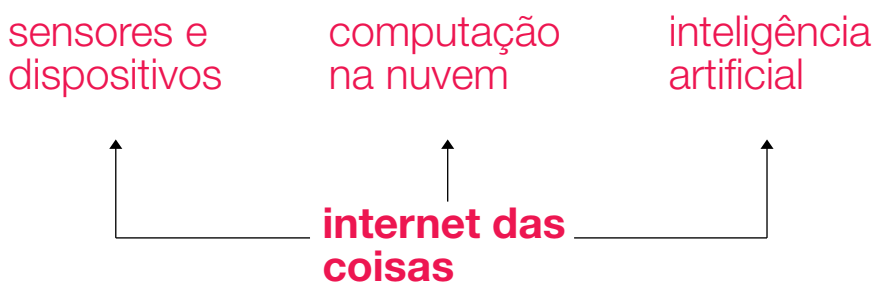
Essa nota se divide em quatro partes. A primeira introduz a IoT e a situa no âmbito político nacional. A segunda analisa três grupos de tecnologias que a sustentam e expõe os principais riscos que apresentam para a privacidade e segurança de sistemas interconectados. A terceira conclui com uma reflexão a respeito dos rumos desse tipo de inovação tecnológica no Brasil. Por fim, traz uma lista de recomendações para formuladores de políticas, com o intuito de contribuir com a definição de normas e princípios basilares para o desenvolvimento da IoT - considerando o conjunto de tecnologias que a constituem e seu papel enquanto projeto político-econômico - e de estratégias digitais mais próximas da realidade do país.

2. Tecnologias emergentes e Internet das Coisas: controvérsias e debates

Na última década, a digitalização e a proliferação de dispositivos de Internet das Coisas (IoT) lançaram luz sobre o potencial econômico e produtivo representado pela integração de sistemas digitais ao setor industrial e - gradualmente - ao cotidiano de consumidores. Aqui, destaca-se três grupos de tecnologias que compõem esse grupo de inovações: sensores e dispositivos, inteligência artificial e computação na nuvem.

13 Sistemas ciber-físicos correspondem a elementos de computação em coordenação e comunicação com sensores. Esses sistemas buscam reunir informações sobre o ambiente a fim de atuar, modificando, o ambiente físico em que são executados. Ver: ZANNI (2015).

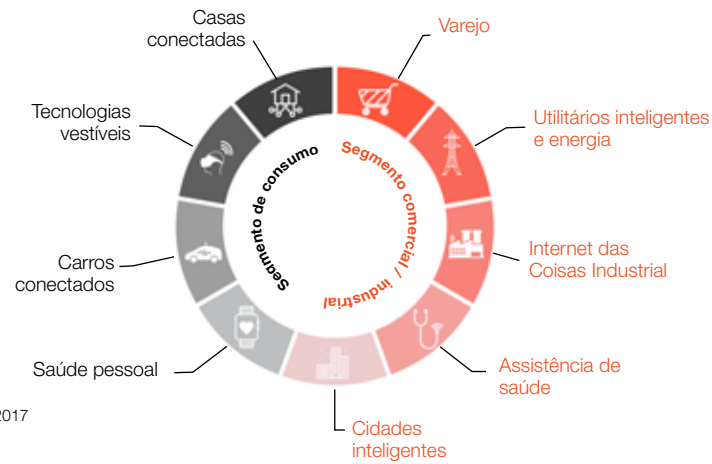
Figura 2: Tecnologias que compõem a IoT



Fonte: desenvolvido pelas autoras.

Estas tecnologias alicerçam o desenvolvimento de uma IoT que visa, simultaneamente, atender consumidores e explorar a digitalização de setores industriais. De um lado, a IoT para consumidores é caracterizada pelo uso de "coisas" e sensores conectados à Internet, como televisores, aparelhos de som, roteadores, automóveis, smartphones, e eletrodomésticos; e é intermediada por serviços diversos, como aplicativos de transporte, aplicativos de tráfego urbano, além de serviços bancários. De outro, a interface comercial e industrial é marcada pela promessa de cidades inteligentes, monitoramento de pacientes em hospitais, aprimoramento na gestão de recursos energéticos e do setor de saúde, entre outros.[14]

Figura 3: Panorama do mercado de IoT



Fonte: Growth Enabler, 2017

14 GROWTH ENABLER (2017).

Os benefícios da implementação da IoT em larga escala são impulsionados pela Indústria 4.0[15] e se respaldam nos seguintes vetores:[16]

- incorporação de sensores a produtos e equipamentos de manufatura;
- proliferação de sistemas ciber-físicos; e
- análise de dados em grande escala.

E são habilitados pelos seguintes processos:

Confluência entre dados, poder computacional e conectividade, o que compreende IoT, computação na nuvem e Big Data. Essa confluência torna possível o uso ubíquo de sensores e uma redução nos custos de processamento transmissão e armazenamento de dados;

Análise e inteligência de dados, possibilitada por avanços na inteligência artificial e aprendizado de máquina (machine learning). Isto favorece processos de digitalização e automação, assim como o desenvolvimento de métodos sofisticados de análise e estatística;

Interação entre humanos e máquinas (*human to machine*), caracterizada principalmente pelo uso de dispositivos pessoais com interfaces sensíveis ao toque, reconhecimento de gestos e realidade aumentada;

Conversão digital-para-o-físico, representada pela robótica avançada e sistemas de impressão 3D. Uma combinação de custos mais baixos, disponibilidade de materiais diversos e avanços na precisão e qualidade são motores desse processo.

O impacto dessas inovações provoca discussões[17] sobre como a Indústria 4.0 traz consigo as sementes para uma "quarta" revolução industrial.[18] Conforme apontado, esta "revolução" depende de um alto grau de convergência tecnológica, da capacidade de processamento e de instrumentos e estruturas físicas (ex.: servidores e sistemas ciber-físicos) para suportar uma verdadeira mudança de paradigma na sociedade e economia de diferentes países.

15 Indústria 4.0, também conhecida como 4ª Revolução Industrial, diz respeito à tendência de automação e troca de dados nas tecnologias do setor da manufatura, incluindo sistemas ciber-físicos, a IoT e tecnologias relacionadas, p.ex., computação na nuvem. O que caracterizaria a Indústria 4.0 seria, sobretudo, a escala e a velocidade da integração de sistemas de TICs a processos industriais. Ver: SCHWAB (2017).

16 MCKINSEY (2015a); MCKINSEY (2015b); HUNG (2017).

17 SCHWAB (2017).

18 Cabe notar que há pouco consenso sobre se, de fato, estamos entrando em uma nova fase de revolução industrial. Nesse sentido, ver: JASPERNEITE (2012).

A controvérsia que se coloca diante desse cenário é a de compreender que essas tecnologias fazem parte do cotidiano das pessoas de uma forma que ainda não percebem, sendo incorporadas a diversos serviços públicos e a gestão do cotidiano urbano.[19] Sendo assim, a pergunta que se coloca é: Quem poderá, de fato, desfrutar dos benefícios da IoT e será que a segurança, mediante as diferentes realidades socioeconômicas entre países, permanecerá central em seu processo de desenvolvimento?

2.1 Contexto: IoT como plano estratégico para o Brasil?

O investimento e integração cada vez maiores dessas tecnologias estão no cerne de disputas geopolíticas e econômicas entre Estados Unidos e Europa. A fim de fazer frente à predominância dos EUA no campo das tecnologias da informação, o bloco europeu anunciou sua própria estratégia de digitalização.[20] No Brasil, esse tipo de estratégia promete avançar com o Plano Nacional de Internet das Coisas, cuja finalidade é a de expandir sua implementação em zonas urbanas e rurais no país, no setor de saúde e na indústria.

Estratégias nacionais de digitalização visam concretizar o potencial econômico da IoT para o desenvolvimento nacional e trazer coerência para uma variedade de iniciativas isoladas no país. No Brasil, isto acontece a partir da Estratégia Brasileira para Transformação Digital (E-Digital) e do Plano Nacional de IoT,[21] que mobiliza órgãos do governo, como Ministério de Ciência, Tecnologia, Inovação e Comunicações (MCTIC), o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), e de pesquisa, como o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD). A elaboração e implementação do Plano foi precedida por um estudo conduzido pela empresa de consultoria McKinsey e pelo CPqD, que identificou oportunidades econômicas para o segmento no país.

Além disso, as estratégias também visam situar o Brasil em meio a grandes agendas internacionais, entre elas os Objetivos de Desenvolvimento Sustentável da Agenda 2030 da ONU. A expectativa é que a E-Digital possa trazer um acréscimo de até 5,7% aos 22% do montante de economia digital do PIB nacional.[22] Essas iniciativas ganharam tração e visibilidade em 2018 e compartilham dois eixos de preocupação relevantes para esse estudo: o mundo de dispositivos conectados e a construção de confiança no ambiente digital.[23]

19 A exemplo do uso de pontuações de crédito (credit scoring, em inglês) pelo setor bancário para determinar taxas de concessão de crédito para clientes (previsto na Lei do Cadastro Positivo), e pontuação de risco (risk scoring, em inglês) pelo poder judiciário para informar execuções penais. Ver: BAWDEN; ANASTÁCIO (2017).

20 DG CONNECT (2017); SAVIN (2014).

21 BUCCO (2017).

22 VALENTE (2018).

23 MCTIC (2018).

Três aspectos fundamentais explicam a centralidade tecnológica da IoT para o desenvolvimento nacional e econômico de diferentes países. Cita-se, em primeiro lugar, a localização da infraestrutura física das "nuvens", cuja integração com dispositivos de IoT possibilita maior capacidade de armazenamento e processamento de dados. Em segundo lugar, com uma variedade de aplicações (agricultura, indústria, cotidiano, administração urbana, medicina e saúde, meio ambiente e outros), a IoT se apresenta como oportunidade real de investimento para diferentes setores da economia, e traz potencial para o desenvolvimento científico. O terceiro aspecto se refere ao potencial para fortalecimento ou enfraquecimento da democracia, na medida em que é possível conceber diferentes formas de engajamento civil ou, alternativamente, de controle social a partir dessa infraestrutura.[24] Exemplos desta ambivalência incluem o uso de mídias sociais para mobilização política e de *bots* tanto para para identificação de notícias falsas quanto para a veiculação de propaganda computacional.[25]

Apesar disso, há desafios significativos relacionados ao crescente uso das IoT e à segurança e privacidade das comunicações e dos indivíduos. Conforme apontado anteriormente, a ampla coleta de dados e a comunicação entre dispositivos se tornaram condições inegociáveis para a realização técnica da IoT. No entanto, a falta de parâmetros claros sobre seu uso pelos provedores de serviço traz sérios problemas relacionados ao uso indevido de dados pessoais por empresas e terceiros. Além disso, a falta de segurança dessas tecnologias facilita ataques cibernéticos em grande escala e roubo de informações pessoais e sensíveis por criminosos. Apenas em 2017, o Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) identificou mais de 800 mil ataques cibernéticos no país, dos quais 53.10% foram varreduras em redes de computadores, feitas com o intuito de "identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles" sendo "amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador."[26] Do total de ataques notificados ao CERT.br em 2017, 220.188 foram ataques de negação de serviço (DoS), dos quais a maioria se originou a partir de equipamentos de IoT infectados e fazendo parte de *botnets*.[27]

Isso ocorre porque, em países como o Brasil, muitos produtos de IoT são desenvolvidos com base em sistemas operacionais e software antigos ou desatualizados.[28] Além disso, há também a falta de critérios e padrões amplamente adotáveis de segurança no desenvolvimento desses dispositivos.[29] No contexto de objetos e aplicações interconectados, o risco de efeitos em cascata relacionados à segurança (ou à falta

24 HOWARD (2015a).

25 HOWARD (2015a); HOWARD (2015b); FATIMABOT (2018).

26 CERT.br (2018a).

27 CERT.br (2018b).

28 COMPUTER WORLD (2016); KURTZ (2017).

29 DUC et al. (2017).

dela) é significativamente ampliado. Para mitigar este problema, deve-se atentar para as tecnologias que alicerçam a IoT e incluir questões associadas à segurança e privacidade em seu design.

3. Desconstruindo a Internet das Coisas

As próximas seções exploram as características, usos e riscos da IoT a partir de uma análise aprofundada das tecnologias que a alicerçam (dispositivos e sensores, computação na nuvem e inteligência artificial).

3.1. Dispositivos e sensores: o que são e quais são os seus riscos?

A IoT pode ser definida como uma rede de sensores que se comunicam e compartilham informações entre si, com o intuito de desempenhar atividades de identificação inteligente, localização, rastreamento, monitoramento e administração de "coisas".[30] Tecnicamente, é composta por elementos de *hardware, middleware* e *software.* O primeiro (*hardware*) se refere aos elementos materiais, como dispositivos e sensores. O segundo (*middleware*) serve como plataforma de integração entre dispositivos, seus sistemas operacionais e diferentes aplicações.[31] Já o terceiro (*software*) informa a funcionalidade do dispositivo e as suas potenciais operações. Sendo assim, a disseminação do uso e o impacto das IoT passam, necessariamente, pela compreensão sobre como essas três camadas são empregadas nos mais diversos espaços, desde a gestão de serviços públicos em uma cidade inteligente, ao uso de um equipamento, como uma *smart TV*, no interior de uma casa.

Compostos por *software* e *hardware*, dispositivos e sensores operam como pontas de captação de dados e são a dimensão mais visível da IoT em virtude de seu caráter material e físico.[32] De acordo com a União Internacional de Telecomunicações (UIT),

30 SUN; WANG (2011).

31 O Middleware reside entre o sistema operacional e as aplicações do dispositivo para assim facilitar a transmissão de dados na realização de uma ou diversas funções programadas no dispositivo. Ver MICROSOFT (s.d.). O debate sobre o papel do middleware em IoT avança com a proliferação de serviços e funcionalidades de dispositivos. Bandyopadhyay et al. (2011), p. 94, argumentam que o objetivo principal do middleware é o de promover interoperabilidade entre dispositivos, servindo a diversos domínios de aplicações.

32 Não existe consenso sobre a definição de IoT, tampouco sobre o papel de dispositivos e sensores. A União Internacional de Telecomunicações (UIT) adota uma definição mais técnica, que considera inclusive, os dispositivos da cadeia de transmissão de dados. Portanto, classifica dispositivos em quatro categorias gerais: dispositivo de transporte de dados, dispositivo de captura, dispositivo de detecção e acionamento e dispositivo geral. Ver UIT (2012), p. 4-5.

"dispositivo" é um pedaço de equipamento com a capacidade de se comunicar e que, opcionalmente, tem capacidade de captação, armazenamento e processamento de dados.[33] Já os sensores permitem o monitoramento, a medição, a coleta e a geração de dados do ambiente (ex: temperatura, propriedades químicas, físicas e/ou biológicas). No contexto de IoT, tais sensores,[34] também chamados de dispositivos de entrada,[35] possuem ampla capacidade de proporcionar novas informações situacionais. Dessa forma, se baseiam em um sistema de retroalimentação e interação entre o serviço providenciado pela "coisa" - ou dispositivo aliado ao sensor - e o ambiente.

O papel de dispositivos e sensores como pontas para a captação de dados se sustenta em dois processos. O primeiro é a comunicação Máquina a Máquina (M2M),[36] ou seja, a interação entre dispositivos conectados à Internet e conectados entre si.[37] Estes objetos formam redes comunicacionais, facilitando o compartilhamento e transmissão de dados, em menor escala (p.ex.: no interior de uma casa ou em atividades específicas) ou maior escala (como em grandes infraestruturas, cidades, etc.).

O segundo diz respeito à comunicação humano e máquina, ou seja, a interação entre o usuário e as funcionalidades programadas dentro de um determinado dispositivo ou ecossistema de sensores. Um exemplo desta interação ocorre quando a ação realizada pelo indivíduo provoca uma resposta do dispositivo, tal como acender a luz, ou programar o despertador.

A M2M e a comunicação entre humano e máquina fazem dos dispositivos partes integrais de uma sociedade mais conectada, em que se observa o emprego de *big data* e a expansão de plataformas capazes de administrar essas redes de "coisas". A promessa da IoT é a de que a proliferação de dispositivos e a possibilidade de captação de dados em massa resultem em uma maior capacidade de conhecer eventos, fenômenos e indivíduos e seus hábitos. Desse modo, parte dos serviços que proporciona se referem à otimização, organização e acesso a novas informações. O impacto econômico esperado da expansão de dispositivos conectados à Internet é de 11 trilhões de dólares até 2025.[38] Entretanto, esse tipo de projeção, aliada ao otimismo que a acompanha, ignoram os riscos reais relacionados à expansão de sensores e dispositivos em ecossistemas de IoT. Destaca-se, a seguir, três preocupações principais:

33 UIT (2012), p. 1.

34 A ENISA (2017), p.19-20, define a funcionalidade de sensores da seguinte forma: "On the physical level, sensors can measure defined physical, chemical or biological indicators, and on the digital level, they collect information about the network and applications. They then generate associated quantitative data, which can be processed in real-time, or stored for later retrieval, and that can be received hundreds of kilometres away. Some examples of sensors are accelerometers, temperature sensors, pressure sensors, light sensors and acoustic sensors, among others".

35 ENISA (2017).

36 Machine to machine, em inglês.

37 CLARK (2016).

38 MANYIKA et al. (2015); PERERA et al. (2015).

3.2 Interoperabilidade e o desafio da padronização

O crescente número de objetos com interfaces, serviços e capacidades computacionais próprias torna a interoperabilidade um elemento fundamental para a integração entre o objeto e seu entorno.[39] No campo da governança da Internet, a interoperabilidade se refere aos mecanismos técnicos operacionais que possibilitam a resiliência e a estabilidade da rede, a exemplo de protocolos e padrões desenvolvidos para roteamento de tráfego online (p.ex.: TLS, BGP, DNSSEC). De modo mais amplo, diz respeito à capacidade de comunicação transparente entre sistemas. Uma rede, produto ou sistema interoperável funciona em conjunto com outras redes, produtos e sistemas, possibilitando assim uma troca fácil de dados e informações.

Uma rede interoperável também torna possível o acesso a páginas web, mesmo quando um dos nodos da rede estiver inoperante, ampliando, por meio de redirecionamento de tráfego, sua resiliência. O uso de padrões técnicos compartilhados é fundamental para a comunicação desimpedida entre sistemas. Em contrapartida, a ausência de padrões compartilhados entre indústria, agências regulatórias, desenvolvedores e provedores é um dos principais obstáculos para a segurança, resiliência e estabilidade da IoT, já que grande parte dos objetos, software e soluções baseiam-se em tecnologias com diferentes padrões técnicos.[40] Para que sejam (inter)conectáveis, esses setores precisam "falar a mesma língua", através de protocolos ou de *gateways,*[41] responsáveis pela harmonização entre sistemas.

3.3 Como garantir a funcionalidade de dispositivos de IoT?

O vasto mercado de IoT engloba serviços e dispositivos com funcionalidades que atendem a demandas variadas, desde o controle integrado das luzes de uma casa até sistemas industriais diversos. Há dois desafios associados ao modo como dispositivos de IoT são programados para desempenhar uma ou mais atividades. Primeiro, deve-se garantir que a performance do objeto não extrapole a funcionalidade para a qual foi designado. Segundo, a coleta e o uso dos dados coletados por esses sensores deve contar com o consentimento livre e expresso dos usuários.

39 A Samsung elencou a multiplicidade de identificadores de objetos como a principal desafio para a segurança da Internet das Coisas em 2018. Ver: ARTIK (2018).

40 Tecnicamente, parte da solução para interoperabilidade se concentra no estabelecimento de gateways, uma espécie de ponte de ligação entre duas ou mais redes, que permitam a harmonização entre diferentes protocolos e sistemas operacionais. Ver: ENISA (2017).

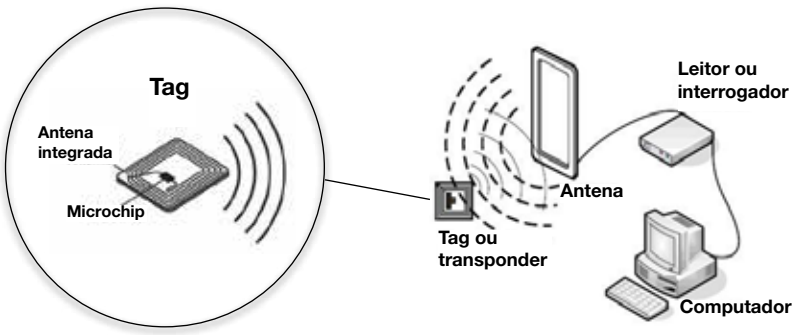
41 ROSE; ELDRIDGE; CHAPIN (2015).

Ao mesmo tempo, a inserção de um objeto em um ambiente de coisas conectadas enseja novos desafios. Entre eles, estão as novas superfícies de ataque, o aumento no número de vulnerabilidades dos sistemas e, no caso de coisas inteligentes, das oportunidades de coleta de dados. Princípios como a minimização de coleta de dados (*data minimization*),[42] o desenvolvimento de softwares que possam ser facilmente atualizados, a exigência de consentimento expresso por parte do usuário, a definição de mecanismos de controle, acesso e portabilidade de dados, e o investimento na segurança durante o ciclo de vida do produto, são fundamentais para a fortalecer a privacidade, proteção de dados e segurança digital.

3.4. Desconectar não é a solução: problemas de segurança offline

Desconectar objetos da Internet pode não ser a solução para a segurança desses ecossistemas. A principal característica de objetos da IoT é sua capacidade de transmitir e receber dados. No entanto, para isto, não necessitam de uma conexão à Internet,[43] ou seja, não dependem de endereçamento IP para se comunicar. Este é o caso de identificadores por radiofrequência (RFID)[44] e Comunicação por Campo de Proximidade (NFC).

Figura 4: Descrição dos componentes e meios de comunicação via RFID



O RFID é um pequeno adesivo identificador utilizado para transmitir dados via comunicação *wireless*. Dado o seu tamanho e finura, o identificador possibilita novas aplicações, tais como o uso de cartões sem chip (*contactless*), chaves de

42 Também incorporado pelo princípio de razoabilidade na coleta de dados, a minimização da coleta é um paradigma mais específico que sustenta a noção de privacidade por concepção. Ver: CAVOUKIAN (2011).

43 ENISA (2017).

44 Em inglês, *Radio Frequency Identification System* (RFID). A RFID é uma tecnologia que auxilia máquinas e computadores na identificação de objetos, guarda de metadados ou controle de determinados objetos por meio de radiofrequência. Ver: JIA et al. (2012), p. 1282.

hotéis, rastreamento de gado, entre outras.[45] No cenário das IoT, essa categoria de identificadores pode ser utilizada para expandir o monitoramento, rastreamento e supervisão de objetos.[46] Um exemplo é o uso de *tags* como medida obrigatória para a indústria automobilística de forma que os identificadores se integrem a sistemas de IoT em cidades e facilitem o monitoramento e estudo de mobilidade urbana.[47]

A segurança de comunicações offline depende de mecanismos de autenticação próprios para este cenário. Respostas incluem, por exemplo, o armazenamento seguro de mensagens direcionadas a dispositivos até que estes possam se conectar à Internet, autenticar-se rede e recebê-las.[48] Contudo, o desafio, para além da comunicação offline, é o de integrar tecnologias e, ao mesmo tempo, impedir que contribuam para vigilância em massa.

Segurança, neste caso, é composta por camadas - *software, hardware, middleware*, - infraestrutura, extremidades da rede e servidores. Agregar diferentes tecnologias operacionais e de informação também significa combinar suas respectivas inseguranças em um novo plano de interação comunicacional (online e offline) por meio da IoT.

3.5 Computação na nuvem: conceitos e desafios

As nuvens são componentes fundamentais da Internet das coisas, materializando-se a partir de vastas "quintas" ou "fazendas" de servidores conectados a redes digitais de alta velocidade.[49] Elas permitem o desenvolvimento de uma variedade de serviços avançados, por meio da interconexão física e virtual das coisas. Têm como base tecnologias de informação e comunicação interoperáveis, além do acesso a um conjunto de recursos computacionais (redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente provisionados com mínimo esforço administrativo ou interação com o provedor do serviço.[50] Plataformas de nuvens de IoT proporcionam o acesso e uso de aplicações, a partir de qualquer lugar do mundo, sem os custos e a complexidade que acompanham a aquisição e administração de elementos de *hardware* e *software* (operando como *middleware*).[51]

45 SHEA (2017).
46 JIA et al. (2012); MIRANI (2014).
47 O'KANE (2018).
48 MICROSOFT (2018).
49 GRAF; HLÁVKA; TRIEZENBERG (2016).
50 RAY (2016); MELL; GRANCE (2011).
51 STERGIOU et al. (2018).

Imagem 1: Quinta de servidores

Foto: Florian Hirzinger

A criação e difusão de novas aplicações de IoT - e os dados produzidos a partir delas - demandam grande poder computacional. Por conta de seu volume, esses dados não podem simplesmente ser transferidos por meio da Internet para serem processados em um só local. Para garantir o fornecimento ininterrupto de serviços de processamento e armazenamento, as "quintas" precisam de ampla distribuição geográfica.[52] Para Wang e Ranjan,[53] um dos principais desafios da distribuição no processamento de dados é justamente o desenvolvimento de mecanismos que possibilitem a segurança e privacidade de dados sensíveis. A integração segura entre a nuvem e dispositivos de IoT é preocupação recorrente entre desenvolvedores e estudiosos dessas tecnologias.[54]

Os problemas de segurança associados à computação na nuvem podem ser encaixados em duas categorias mais amplas. A primeira é relativa a questões de segurança enfrentadas pelos *provedores do serviço*, os quais necessitam de uma infraestrutura segura para comunicação e armazenamento de dados. A segunda se refere aos problemas enfrentados pelos *consumidores* que armazenam aplicações ou dados na nuvem, que carecem da adoção de senhas e medidas de autenticação robustas.[55] Além desses, cita-se os desafios referentes à

52 A distribuição geográfica de servidores alimenta uma série de questões geopolíticas sobre, entre outros, sua alocação, bem como as condições de acesso aos dados neles armazenados. Ver, por exemplo: SIMON (2017); BURRINGTON (2015); URQUHART (2010); DIMAIO (2009).

53 WANG; RANJAN (2015).

54 STERGIOU et al. (2018); HUTH; CEBULA (2011).

55 STERGIOU et al. (2018).

integração entre nuvens e IoT, a exemplo da falta de confiança no provedor de serviços, o (des) conhecimento sobre a localização física dos dados e os Acordos de Nível de Serviços,[56] e a restrição de aplicação de chaves públicas de criptografia devido a limitações computacionais.

Ao subscrever a um serviço de nuvem, o usuário - individual ou comercial - abre mão de uma parcela do controle que tem sobre os seus dados para um terceiro.[57] Dessa forma, torna-se dependente das medidas de segurança adotadas pelos provedores do serviço que utiliza. Entre estas, destaca-se o estabelecimento de padrões de criptografia de dados, medidas de proteção do *hardware* onde os dados são armazenados, além do uso de cópias de segurança dos dados, ou *backup*, e *firewalls,*[58] que assegurem que estes estejam protegidos do acesso indevido e indiscriminado de terceiros e de quaisquer possibilidade de perda. A adoção de medidas mais robustas aumenta o nível de segurança da nuvem, ao passo que brechas e vulnerabilidades nas medidas adotadas podem favorecer acessos não autorizados aos dados nela armazenados e, consequentemente, seu roubo e uso indevido.

3.6. Decisões automatizadas e coisas 'inteligentes'

O emprego de decisões automatizadas, através da incorporação de tecnologias de aprendizado de máquina e inteligência artificial, potencializa e facilita o surgimento de novas funções e mercados para a IoT. Conforme apontado por Mayer-Schönberger e Cukier,[59] a viabilização da IoT como promessa de otimização social e econômica se respalda no que chamam de datafication,[60] ou seja, a quantificação de hábitos, comportamentos e ações para que sejam analisados, relacionados e reorganizados.

A aplicação dessas tecnologias se dá em diferentes escalas. Em menor escala, envolve seu uso no ambiente doméstico, por meio de assistentes pessoais como a Alexa (Amazon) e a Siri (Apple). Já o uso em larga escala diz respeito à manutenção e operação de infraestruturas críticas, como redes elétricas, telecomunicações e sistemas de transporte.[61]

A construção de casas conectadas e integradas a sistemas de inteligência artificial contribui também para o reposicionamento da tecnologia como parte integral do dia a dia. Estabelece, assim, um sistema baseado na "dataficação" de atividades cotidianas, no qual os fluxos de dados são majoritariamente regidos por termos de uso e de serviço.

---

56 Trata-se de um compromisso assumido por um prestador de serviços de TI perante um cliente e que descreve o serviço de TI a serem prestados, os níveis de qualidade a serem garantidos, as responsabilidades das partes e eventuais compensações quando os níveis de qualidade não forem atingidos.

57 HUTH; CEBULA (2011).

58 Firewalls são dispositivos ou aplicativos que monitoram o fluxo de dados em uma rede, autorizando ou bloqueando estes fluxos de acordo com um conjunto definido de regras de segurança.

59 MAYER-SCHÖNBERGER; CUKIER (2013).

60 De acordo com Mayer-Schönberger e Cukier (2013), p.97, "[t]o datafy a phenomenon is to put it in a quantified format so it can be tabulated and analyzed".

61 A cidade de Santander, na Espanha, ilustra o uso de IoT em grande escala, sendo considerada um dos principais experimentos internacionais de cidade inteligente. Em Santander, as parcerias com grandes empresas de tecnologia permitiram integrar, monitorar e aprimorar mais de 20.000 sensores que quantificam fluxos de tráfego, níveis de poluição e ruídos, temperatura e cronograma de transportes públicos diários na cidade. Já os assistentes pessoais que se utilizam de sistemas operacionais baseados na Inteligência Artificial trabalham e aprendem com base nos dados que coletam, bem como servem como plataformas de integração entre lâmpadas, relógios, eletrodomésticos e chuveiros inteligentes.

No entanto, o crescente recurso a coisas inteligentes chama a atenção para a importância de se desenvolver mecanismos de responsabilização para a coleta e tratamento de dados, facilitando o acesso de usuários às informações que plataformas e empresas acumulam a seu respeito. Além disso, é importante a garantia a um "direito à explicação"[62] sobre como determinado algoritmo alcançou um resultado específico.

4. Privacidade e segurança por concepção: integrando dispositivos, políticas e diretrizes

Aprovada no dia 14 de agosto de 2018, Lei de Proteção de Dados Pessoais (LPDP)[63] brasileira coloca a privacidade e segurança como princípios basilares para a proteção de dados no país. Além disso, também obriga os agentes de tratamento de dados[64] a adotarem medidas técnicas e administrativas de segurança para proteger dados pessoais, particularmente no que diz respeito a acessos não-autorizados e situações acidentais ou ilícitas de destruição, perda, alteração e comunicação.[65] Enquanto a lei oferece importante fundamento para o avanço da IoT no país, é necessário, ainda, que esses princípios sejam efetivamente incorporados ao desenvolvimento dessas tecnologias e que se desenhe mecanismos mais robustos de estímulo ao investimento nesse processo. Um ponto de partida é encontrar um equilíbrio entre a concepção de tecnologias seguras, potenciais diretrizes que pautam o seu desenvolvimento e políticas de estímulo à sua adoção.

Denomina-se *privacidade por concepção* e *segurança por concepção* a necessidade de se incluir privacidade e segurança no desenvolvimento de plataformas digitais, sistemas e softwares.[66] *Privacidade por concepção* compreende tanto a implementação de regulações e princípios (minimização na coleta de dados, consentimento informado, notificação, acesso, escolha e segurança)[67] quanto técnicas para minimizar a coleta de dados pessoais - as chamadas "tecnologias para melhorar a privacidade" (PETs, em inglês).[68] Estas podem ser divididas em duas categorias: substitutivas e complementares.

62 GOODMAN; FLAXMAN (2016); SELBST; POWLES (2017).

63 BRASIL (2018).

64 Pela Lei, são agentes de tratamento aqueles que decidem sobre - ou realizam, de fato - o tratamento de dados pessoais.

65 Artigo 46 da Lei de Proteção de Dados Pessoais.

66 CAVOUKIAN (2011); DOUGHERTY et al. (2009).

67 SPIEKERMANN; CRANOR (2009).

68 É importante ressaltar que embora intercambiável, o conceito de PET não se confunde com o de privacidade por concepção. As PETs são aplicações ou ferramentas que se endereçam a uma dimensão da privacidade, por exemplo, anonimato, confidencialidade ou controle sobre a informação pessoal. Já a privacidade por concepção é uma categoria ampla e sistemática que aborda como uma tecnologia deve ser desenhada de modo a embutir "privacidade" em suas especificações básicas e de arquitetura. A privacidade por concepção pode, dessa forma, tanto dizer respeito a um conjunto de práticas dentro de uma organização quanto a um sistema computacional.

- As *substitutivas* são responsáveis por bloquear ou minimizar a coleta de dados pessoais; apoiando-se tanto no anonimato quanto em arquiteturas que priorizam a identificação do usuário (centradas no usuário).[69] Este é o caso de ferramentas como a rede Tor, e-mails criptografados e janelas de navegação anônima.
- Já as *complementares* são mais receptivas à coleta de dados - desde que sejam consistentes com regulações para a proteção à privacidade. Esse tipo de medida visa a redução do risco de danos ao cliente. É o caso de mecanismos de consentimento informado, administração de preferências e direitos de acesso, assim como técnicas de mineração de dados e propaganda direcionada que preservam a privacidade.[70]

Já a *segurança por concepção* requer a adoção, ainda na fase de desenvolvimento, de medidas que tornem sistemas e softwares mais seguros contra ataques cibernéticos e preservem a integridade e a confidencialidade das informações que armazenam e processam.[71] Exemplos incluem a adoção e desenvolvimento de protocolos (como IPv6, TLS e HTTPS) e de arquiteturas seguras,[72] minimização da superfície de ataque,[73] adoção de padrões seguros (como o uso de prazos de expiração para senhas e de senhas complexas) e uso de mecanismos de segurança "em camadas".[74]

A introdução dessas duas abordagens permite a conciliação entre segurança e privacidade enquanto conceitos e prerrogativas para o desenvolvimento operacional de tecnologias associadas à IoT. Estes aprimoramentos técnicos são apenas um aspecto da segurança e privacidade por concepção. É também fundamental que diferentes setores adotem medidas de caráter administrativo com o intuito de estimular boas práticas de proteção de dados, privacidade e segurança. Alguns exemplos incluem a emissão de certificados, programas corporativos, relatórios de impacto e códigos de boa conduta. Além disso, embutir ambos os princípios no desenho institucional - e não apenas no produto - é fundamental para garantir que a segurança e a privacidade sejam, de fato, incorporadas às práticas e à cadeia de produção da organização, desde a concepção à execução do projeto.[75]

A gestão desses processos inclui as seguintes considerações: a escolha responsável de provedores de serviço e componentes de terceiros; o estabelecimento de planos de gestão de riscos de segurança do produto; a realização de avaliações de riscos de segurança do produto para detecção de softwares maliciosos e/ou defeitos; e o planejamento de redução e mitigação de riscos.

---

69 Outros exemplos podem ser encontrados em: ZUCKERMAN (2005).

70 MENDES; VILELA (2017); TOUBIANA et al. (2010).

71 REDALERTLABS (2018).

72 Uma aplicação cuja arquitetura é segura deve proporcionar controles que protejam a confidencialidade da informação (ou seja, que o usuário acesse apenas informações para as quais está autorizado), sua integridade (assegurar que os dados ou informações não sejam indevidamente utilizadas ou modificadas) e disponibilidade para os usuários adequados, quando o acesso solicitado.

73 Uma superfície de ataque corresponde à soma das vulnerabilidades em um dispositivo ou rede que os tornam vulneráveis a ataques cibernéticos. Cada novo recurso adicionado aumenta a superfície de ataque e, com ela, os riscos de ataques. Denomina-se desenvolvimento seguro as tentativas de reduzir estes riscos, por exemplo, centralizando rotinas de validação, limitando acesso ao(s) recurso(s) a usuários autorizados, entre outros.

74 Trata-se da implementação de diferentes mecanismos de segurança que tornam possível a "reação" de um sistema, mesmo quando um dos mecanismos venha a falhar.

75 DE LA CÁMARA et al. (2016).

Tabela 1: Ecossistema para a regulação para IoT baseado na privacidade e segurança desde a concepção.

Natureza	Técnica	Regulatória e governança	Administração e gestão
Exemplos	PETs, uso de protocolos seguros (IPv6, TLS, HTTPS e MQTT), minimização da superfície de ataque, prazos de expiração para senhas por padrão, criptografia em serviços de nuvem, segurança por "camadas", respostas a incidentes, etc.	Regulação: Lei nº 13.709, de 14 de agosto de 2018 (LPDP), Plano Nacional de IoT, Código de Defesa do Consumidor, Lei de Acesso à Informação, Decreto 8.234 de 02 de maio de 2014 (regulação M2M). Portaria 1.729 de 31 de março de 2017 MCTIC (Estabelece a Câmara IoT, órgão multissetorial). Governança: Colaboração entre diferentes setores[1] e a autoridade de supervisão para a determinação de necessidades e riscos referentes às tecnologias de IoT.	Assegurar o respaldo de setores de chefia; estandardizar processos de desenvolvimento seguro; gerenciar vulnerabilidades e segurança de projetos.
Objetivo	Garantir que hardware, software e middleware sejam seguros (resilientes contra ataques cibernéticos, preservando a integridade e confidencialidade das informações que processam) desde sua concepção e desenvolvimento.	Estabelecer princípios basilares para o desenvolvimento da IoT no país; regular a coleta e o uso de dados pessoais; garantir segurança jurídica; facilitar a coordenação inter-setorial; estimular a adoção de boas práticas; definir e aplicar penalidades.	Tornar o ambiente institucional favorável à adoção de medidas técnicas de reforço da privacidade e segurança; garantir que esses princípios sejam incorporados em toda a cadeia da organização (p.ex, para além da tecnologia).
Desafios	Criar estímulos positivos[2] para que empresas, engenheiros e desenvolvedores adotem tecnologias seguras na prática.	Criar uma autoridade de proteção de dados independente e mecanismos de responsabilização e explicação; desenvolver uma jurisprudência sobre a interpretação da LPDP; realizar diálogos contínuos entre governo, sociedade civil e empresas para viabilizar a aplicação de medidas técnicas e administrativas; harmonizar a LPDP e a estratégia de transformação digital do governo e o Plano Nacional de IoT.	Conscientizar organizações sobre os custos de produtos e serviços inseguros, criar incentivos e formular estratégias para a adoção em escala da privacidade e segurança desde a concepção.

Fonte: Elaboração das autoras.

A Tabela 1 ilustra o funcionamento de um ecossistema de governança da IoT pautado nos princípios da privacidade e da segurança por concepção. Não se diferencia entre medidas que incrementam segurança e privacidade, pois se considera ambas como complementares e necessárias para o funcionamento desse ecossistema. Este é composto por três dimensões específicas:

- A primeira é a *dimensão técnica*, caracterizada pela adoção de padrões e medidas que visam aumentar a segurança de sistemas, softwares e máquinas, o que inclui a proteção aos dados e informações neles coletados, processados e armazenados.

- A segunda é *regulatória e de governança*, abarcando leis, normativas, diretivas, assim como arranjos colaborativos entre diferentes setores envolvidos no desenvolvimento e avanço da IoT no país.

- Por fim, a terceira dimensão envolve medidas de *administração e gestão*, ou seja, iniciativas e mudanças organizacionais que visam assegurar o desenvolvimento de uma IoT mais seguro.

Aponta-se a dificuldade em se implementar aspectos importantes da segurança da informação e privacidade ao contexto da IoT.[76] De modo mais específico, a prática de gerenciamento de dados - crucial para a expansão da IoT - lida com duas questões centrais: como manter seguros os dados e informações processados e como garantir que permaneçam sob o controle de seu dono legítimo. O primeiro desafio é implementar técnicas que reforcem a segurança e a privacidade dos dados e sistemas que os processam, como gerenciamento de confiança medidas de autenticação, administração de chaves, controle do uso de dados e respostas a incidentes, por exemplo. Apesar de amplamente debatidos do ponto de vista conceitual, há pouca aderência por parte dos engenheiros à incorporação da privacidade e segurança a sistemas e softwares.[77] O segundo é a construção de um ecossistema sustentável, que compreenda tanto o desenvolvimento de tecnologias seguras, do ponto de vista técnico, quanto a definição de processos que estimulem e certifiquem boas práticas de segurança e privacidade.

A adoção conjunta dessas medidas é central para a incorporação dos princípios da *privacidade e segurança por concepção* nas tecnologias e organizações. O ecossistema regulatório é atualmente constituído por um conjunto de normas setoriais (por exemplo, Código de Defesa do Consumidor, Marco Civil da Internet) e a Lei de Proteção de Dados Pessoais - e, futuramente, incluirá o Plano Nacional de Internet das Coisas. Além dessas, é importante promover a colaboração entre diferentes setores e a autoridade de supervisão, a qual incumbiria a aplicação de obrigações legais e o estímulo a boas

76 BARBOSA et al. (2017).

77 SPIEKERMANN; CRANOR (2009); HUSTINX (2010); GÜRSES; TRONCOSO; DIAZ (2011).

práticas. Assim, as necessidades e riscos referentes às tecnologias de IoT são definidos levando em consideração as demandas e realidades de cada setor. No entanto, é necessário que haja diálogos contínuos e concretos entre os setores interessados, capazes de viabilizar a incorporação prática desse conjunto de medidas.

5. Considerações finais e recomendações

A IoT é hoje um novo paradigma para a Internet, sendo moldada por um conjunto específico de tecnologias emergentes. No entanto, o rápido crescimento no número de dispositivos interconectados e sua difusão no mercado apresentam desafios tecnológicos, políticos e sociais. O principal deles consiste na pouca importância atribuída à privacidade e à segurança por concepção. Assim, o reconhecimento do potencial econômico desse novo momento tecnológico não veio acompanhado de uma discussão sobre *como* essas tecnologias vêm sendo desenvolvidas, nem sobre as medidas de segurança e proteção que são necessárias.

Uma vez assinado, o Plano Nacional de IoT trará maior ênfase à inserção de tecnologias IoT no âmbito de cidades, saúde e agricultura e agropecuária. É fundamental que a implementação do Plano leve em consideração não só o entusiasmo com relação à digitalização desses setores, mas considere que a falta de atenção às características e riscos apresentados por tecnologias como dispositivos, nuvens e inteligência artificial é um entrave ao desenvolvimento de mecanismos regulatórios e de gestão seguros e interoperáveis.

A partir das análises realizadas sobre os riscos dessas tecnologias, recomenda-se:

Fortalecer o sistema de governança para IoT, ou seja, a interlocução entre desenvolvedores, empresas, consumidores e formuladores de políticas, particularmente no que diz respeito à: (i) Consolidação (técnica e regulatória) de valores que devem reger a fabricação, comercialização e implementação de sensores; e (ii) Proteção dos dados e privacidade de seus usuários.

Garantir a representação da sociedade civil é fundamental para garantir a continuidade, legitimidade e avanço de políticas públicas nessa área.

Definir mecanismos que assegurem a eficácia da Lei Geral de Proteção de Dados Pessoais, que incluem o estabelecimento de um regime de responsabilidade eficaz e de um mecanismo de governança pautado na criação de uma autoridade

independente para a proteção de dados pessoais.

Definir os princípios que devem guiar o desenvolvimento e ampliação da IoT no país, entre os quais destacamos segurança e privacidade por concepção.

Estabelecer padrões mínimos de segurança e interoperabilidade entre sistemas, o que inclui a criação de incentivos positivos e a inserção de valores no desenvolvimento dessas tecnologias, tais como confiança, transparência, segurança por padrão e por concepção. Desenvolvedores, autoridades reguladoras e possíveis implementadores devem estabelecer períodos de validade para os dispositivos, de modo a garantir a segurança do usuário; emitir certificados que indiquem que aquela tecnologia adere a um determinado nível padrão de segurança e privacidade e assim; repensar formas de comunicar riscos e com o consumidor.

Investir, no âmbito dos municípios, na capacitação de servidores para os temas de proteção de dados pessoais, segurança cibernética e da informação, já que eles tendem a ser diretamente responsáveis pela implementação, em larga escala, de tecnologias de sensores.

Garantir a inserção efetiva do governo no debate, na medida em que diferentes esferas estão implicadas em estratégias de planejamento e/ou implementação dessas tecnologias, bem como no desenvolvimento de padrões operacionais.

Investir e ampliar a capacitação da sociedade para entender a importância da agenda de proteção de dados pessoais na era da Internet das coisas, para possibilitar maior engajamento público na definição de pontos importantes da agenda.

Incluir as comunidades locais na elaboração de políticas públicas para a IoT, sistemas e redes urbanas de sensores, a fim de que essas tecnologias sirvam às mesmas e compreendendo que a implementação estratégica efetiva e benéfica da Internet das Coisas no Brasil deve atender à diversidade local e regional do país.

Principais siglas

IA - Inteligência Artificial

IoT - Internet das coisas

M2M - Comunicação Máquina a Máquina, *Machine to Machine*, em inglês

NFC - Comunicação por Campo de Proximidade, *Near-Field Communication*, em inglês

RFID - Identificação por Radiofrequência, *Radio Frequency Identification System*, em inglês

TICs - Tecnologias da Informação e Comunicação

Instituições

BNDES - Banco Nacional de Desenvolvimento Econômico e Social

CERT.br - Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil

CPqD - Centro de Pesquisa e Desenvolvimento em Telecomunicações

MCTIC - Ministério da Ciência, Tecnologia, Inovações e Comunicações

NIST - National Institute of Standards and Technologies

UIT - União Internacional de Telecomunicações

Referências

ABBATE, J. (1999). *Inventing the Internet*. Cambridge: The MIT Press.

ANATEL (2017). *Relatório anual*. Disponível em: http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=348421&pub=original&filtro=1&documentoPath=348421.pdf. Acesso em: 09 out. 2018.

ARTIK (2018). "Top three IoT security trends to watch in 2018". Samsung ARTIK. Disponível em: https://www.artik.io/blog/2018/01/top-three-iot-security-trends-watch-2018/. Acesso em 16 jun. 2018.

BARBOSA, M. et al (2017). "Safethings: Data security by design in the IoT". 13th European Dependable Computing Conference, Geneva, 2017, p. 117-120.

BANDYOPADHYAY, S. et al (2011). "Role of middleware for Internet of Things: a study". International Journal of Computer Science and Engineering Survey, vol. 2, n. 3, p. 95-105. Disponível em: https://www.researchgate.net/publication/266287969_Role_Of_Middleware_For_Internet_Of_Things_A_Study. Acesso em: 10 jun. 2018.

BAWDEN, H.; ANASTÁCIO, K. (2017). Credit Scoring no Brasil. JOTA. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/credit-scoring-no-brasil-26012017. Acesso em: 6 nov. 2018.

BNDES (s.d). *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: 26 jun. 2018.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em 16 ago. 2018.

BUCCO, R. (2017). "Plano nacional de IoT entra em execução". Telesíntese. Disponível em: http://www.telesintese.com.br/plano-nacional-de-iot-entra-em-fase-de-execucao/. Acesso em: 12 jun. 2018.

BURRINGTON, I. (2015). "The strange geopolitics of the international cloud". The Atlantic. Disponível em: https://www.theatlantic.com/technology/archive/2015/11/the-strange-geopolitics-of-the-international-cloud/416370/. Acesso em 10 jun. 2018.

CAVOUKIAN, A. (2011). “Privacy by design in law, policy and practice: a white paper for regulators, decision-makers and policy-makers”. Information and Privacy Commissioner, Ontario. Disponível em: http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf. Acesso em: 1 de jul de 2018.

CERT.br. (2018a). *Estatísticas dos Incidentes Reportados ao CERT.br*. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 22 out. 2018.

CERT.br. (2018b). Incidentes Reportados ao CERT.br - janeiro a dezembro de 2017. Disponível em: https://www.cert.br/stats/incidentes/2017-jan-dec/analise.html. Acesso em: 22 out. 2018.

CETIC.br (2017). TIC Domicílios 2017. CETIC.br. Disponível em: https://www.cetic.br/pesquisa/domicilios/. Acesso em: 31 out 2018.

CLARK, J. (2016). “What is M2M technology?”. IBM. Disponível em: https://www.ibm.com/blogs/internet-of-things/what-is-m2m-technology/. Acesso em: 10 jun. 2018.

COMPUTER WORLD (2016). “Sistemas desatualizados são a principal vulnerabilidade crítica no Brasil”. Computer World. Disponível em: https://computerworld.com.br/2016/10/18/sistemas-desatualizados-sao-principal-vulnerabilidade-critica-no-brasil/. Acesso em 20 jul. 2018.

DE LA CÁMARA, M.; SÁENZ-MARCILLA, J.; ARCILLA-COBIÁN, M.; CALVO-MANZANO, J. (2016). Prácticas de seguridad por diseño para la gestión de proyectos TI en PYMEs. 11ª Conferencia Ibérica de Sistemas y Tecnologías de Información, 15-18 de junio de 2016, Gran Canaria, Islas Canarias, España.

DG CONNECT (2017). “Digital single market: Europe 2020 strategy”. European Commission. Disponível em: https://ec.europa.eu/digital-single-market/en/europe-2020-strategy. Acesso em: 15 mai. 2018.

DE ROECK, D. (2018). “IoT and Value. A dangerous game”. The State of Responsible IoT 2018. ThingsCon. Disponível em: https://www.thingscon.com/blog/2018/08/report-the-state-of-responsible-iot-2018. Acesso em: 01 nov. 2018.

DIMAIO, A. (2009). “The geopolitics of cloud computing”. Gartner Blog Network. Disponível em: https://blogs.gartner.com/andrea_dimaio/2009/08/17/the-geopolitics-of-cloud-computing/. Acesso em 10 jun. 2018.

DOUGHERTY, C. et al (2009). “Secure design patterns (CMU/SEI-2009-TR-010)”. Carnegie Mellon University. Disponível em: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9115. Acesso em: 10 ago. 2018.

DUC, A. N. et al (2017). “Security challenges in IoT development: A software engineering perspective”. XP’17 Workshops. Disponível em: https://www.researchgate.net/publication/319132115_Security_challenges_in_IoT_development_a_software_engineering_perspective. Acesso em: 22 de out. 2018.

ENISA (2017). “Baseline security recommendations for IoT in the context of critical information infrastructures”. Enisa. Disponível em: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. Acesso em: 9 jun. 2018.

FATIMABOT (2018). Disponível em: https://twitter.com/fatimabot. Acesso em 08 ago. 2018.

GOODMAN, B.; FLAXMAN, S. (2016). “European Union regulations on algorithmic decision-making and a ‘right to explanation’”. ICML Workshop on Human Interpretability in Machine Learning. Disponível em: https://arxiv.org/abs/1606.08813. Acesso em: 23 jun. 2018.

GRAF, M.; HLAVKA, J. P.; TRIEZENBERG, B. L. (2016). “A change is in the air: emerging challenges for the cloud computing industry”. Santa Monica: RAND. Disponível em: https://www.rand.org/pubs/working_papers/WR1144.html. Acesso em: 13 jun. 2018.

GROWTH ENABLER (2017). *Market pulse report, Internet of Things (IoT)*. Disponível em: https://growthenabler.com/reports/IOT.html. Acesso em: 02 out. 2018.

HOWARD, P. (2015a). “Politics won’t know what hit it: The Internet of things is poised to change democracy itself.”. Politico. Disponível em: https://www.politico.com/agenda/story/2015/06/philip-howard-on-iot-transformation-000099. Acesso em: 14 jun. 2018.

HOWARD, P. (2015b). “Civic engagement, bots, and the Internet of Things (IoT)”. Oxford Internet Institute. Disponível em: https://www.oii.ox.ac.uk/videos/civic-engagement-bots-and-the-internet-of-things-iot/. Acesso em: 08 ago. 2018.

HUNG, M. (2017). “Leading the IoT: Gartner insights on how to lead in a connected world”. Gartner. Disponível em: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf. Acesso em: 1 out. 2018.

HUSTINX, P. (2010). “Privacy by design: delivering the promises”. Identity in the Information Society, vol. 3, n. 2, p. 253–255. Disponível em: https://link.springer.com/article/10.1007/s12394-010-0061-z#citeas. Acesso em: 16 ago. 2018.

HUTH, A.; CEBULA, J. (2011). “The basics of cloud computing”. US CERT. Disponível em: https://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf. Acesso em: 14 jun. 2018.

JASPERNEITE, J. (2012). “Was hinter Begriffen wie Industrie 4.0 steckt”. Computer & Automation. Disponível em: https://www.computer-automation.de/steuerungsebene/steuern-regeln/artikel/93559/0/. Acesso em: 15 mai. 2018.

JIA, X. et al. (2012). “RFID Technology and its applications in Internet of Things (IoT)”. IEEE. p.1282-1285. Disponível em: https://ieeexplore.ieee.org/document/6201508/. Acesso em 16 jun. 2018.

KITCHIN, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*. London: SAGE Publications.

KOLIAS, C. et al. (2017). “DDoS in the IoT: Mirai and other botnets”. Computer, vol. 50, n.7, p.80-84. Disponível em: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7971869&isnumber=7971854. Acesso em: 6 de ago. 2018.

KURTZ, J. (2017). “Um em cada cinco dispositivos IoT no Brasil é vulnerável, diz pesquisa”. TechTudo. Disponível em: https://www.techtudo.com.br/noticias/2017/08/um-em-cada-cinco-dispositivos-iot-no-brasil-e-vulneravel-diz-pesquisa.ghtml. Acesso em 8 ago. 2018.

MANYIKA, J et al. (2015). “Unlocking the potential of the Internet of Things”. McKinsey Digital. Disponível em: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. Acesso em: 16 jun 2018.

MAYER-SCHÖNBERGER, V.; CUKIER, K. (2013). *Big Data: a revolution that will transform how we live, work and think*. London: John Murray.

MCKINSEY (2015a). “Industry 4.0: How to navigate digitization of the manufacturing sector”. McKinsey & Company. Disponível em: https://www.mckinsey.com/business-functions/operations/our-insights/industry-four-point-o-how-to-navigae-the-digitization-of-the-manufacturing-sector . Acesso em: 13 jun. 2018.

MCKINSEY (2015b). “The Internet of Things: Mapping the value beyond the hype”. McKinsey & Company. Disponível em: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx. Acesso em: 01 out. 2018.

MCTIC (2017). “Brasil já tem 20 milhões de conexões inteligentes entre máquinas”. Governo do Brasil. Disponível em: http://www.brasil.gov.br/noticias/educacao-e-ciencia/2017/02/brasil-ja-tem-20-milhoes-de-conexoes-inteligentes-entre-maquinas. Acesso em: 02 de out. 2018.

MCTIC (2018). “Estratégia brasileira para a transformação digital”. Governo do Brasil. Disponível em: http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf. Acesso em: 02 out. 2018.

MELL, P.; GRANCE, T. (2011). “The NIST definition of cloud computing: recommendations of the National Institute of Standards and Technology”. US Department of Commerce. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Acesso em: 30 mai. 2018.

MENDES, R.; VILELA, J.P. (2017). “Privacy-preserving data mining: methods, metrics, and applications”. IEEE Access, vol. 5, p. 10562-10582. Disponível em: https://ieeexplore.ieee.org/document/7950921/. Acesso em 13 ago. 2018.

MICROSOFT (s.d.). “What is middleware?”. Microsoft Azure. Disponível em: https://azure.microsoft.com/en-gb/overview/what-is-middleware/. Acesso em: 9 jun. 2018.

MICROSOFT (2018). *Microsoft Azure IoT reference architecture*. Disponível em: Microsoft Azure IoT Reference Architecture - Microsoft Download Centerdownload.microsoft.com/.../Microsoft_Azure_IoT_Reference_Ar…. Acesso em: 22 out. 2018.

MINERVA, R.; BIRU, A.; ROTONDI, D. (2015). “Towards a definition of the Internet of Things (IoT)”. IEEE. Disponível em: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf. Acesso em: 20 jul. 2018.

MIRANI, L. (2014). The ‘Internet of Things’ may not always need an internet connection. Quartz. Disponível em: https://qz.com/228750/the-internet-of-things-may-not-need-an-internet-connection/. Acesso em 16 jul. 2018.

O’KANE, S. (2018). China wants to track citizens’ cars with mandatory RFID chips. The Verge. Disponível em: https://www.theverge.com/2018/6/13/17458432/china-surveillance-car-tracking-mandatory-rfid-chips. Acesso em: 1 nov 2018.

PERERA, C. ET AL(2015). “Big data privacy in the Internet of things era”. IEEE. Disponível em: https://ieeexplore.ieee.org/document/7116422/. Acesso em: 12 jun. 2018.

RAY, P. P. (2016). “A survey of IoT cloud platforms”. Future Computing and Informatics Journal, vol. 1, n. 1–2, p. 35-46. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167739X1630694X?via%3Dihub. Acesso em: 13 jun. 2018.

REDALERTSLABS (2018). “The importance of security by design for IoT devices”. Red Alert Labs. Disponível em: https://www.redalertlabs.com/blog/the-importance-of-security-by-design-for-iot-devices. Acesso em: 20 ago. 2018.

ROSE, K.; ELDRIDGE, S.; CHAPIN, L. (2015). “The Internet of things: An overview”. Internet Society. Disponível em: https://www.internetsociety.org/resources/doc/2015/iot-overview. Acesso em: 12 jun. 2018.

SAVIN, A. (2014). “How Europe formulates internet policy”. Internet Policy Review, vol. 3, n.1. Disponível em: https://policyreview.info/articles/analysis/how-europe-formulates-internet-policy. Acesso em: 15 mai. 2018.

SCHWAB, K. (2017). *The fourth industrial revolution.* Nova York: Crown Business.

SELBST, A. D.; POWLES, J. (2017). “Meaningful information and the right to explanation.” International Data Privacy Law, vol. 7, n. 4, p. 233-242. Disponível em: https://academic.oup.com/idpl/article/7/4/233/4762325. Acesso em: 27 jun. 2018.

SHEA, S. (2017). “RFID (Radio Frequency Identification)”. Tech Target. Disponível em: https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification. Acesso em; 09 de out 2018.

SIMON, T. (2017). “The Geopolitics behind the cloud data centers”. Digital Culturist. Disponível em: https://digitalculturist.com/the-geopolitics-behind-the-cloud-data-centers-b1c424d874b6. Acesso em: 10 jun. 2018.

SPIEKERMANN, S.; CRANOR, L. F. (2009). “Engineering privacy”. IEEE Transactions on Software Engineering, vol.35, n.1. Disponível em: https://ieeexplore.ieee.org/document/4657365/. Acesso em 13 ago. 2018.

STERGIOU, C. et al. (2018) “Secure integration of IoT and cloud computing”. Future Generation Computer Systems, vol. 78, p. 964-975. Disponível em: http://www.sciencedirect.com/science/article/pii/S0167739X1630694X. Acesso em: 13 jun. 2018.

TOUBIANA, V. et al (2010). *Adnostic: Privacy preserving targeted advertising*. Disponível em: https://crypto.stanford.edu/adnostic/adnostic.pdf. Acesso em 13 ago. 2018.

UIT (2012). “Series Y: Global Information Infrastructure, Internet Protocols Aspects and Next-Generation Networks”. International Telecommunications Union. Disponível em: https://www.itu.int/rec/T-REC-Y/en. Acesso em: 10 jun. 2018.

URQUHART, J. (2010). “The cloud cannot ignore geopolitics”. CNET. Disponível em: https://www.cnet.com/news/the-cloud-cannot-ignore-geopolitics/. Acesso em: 10 jun. 2018.

VALENTE, J. (2018). “Programa propõe ações para transformação digital na economia”. Agência Brasil. Disponível em: http://agenciabrasil.ebc.com.br/pesquisa-e-inovacao/noticia/2018-03/programa-propoe-acoes-para-transformacao-digital-na-economia. Acesso em: 22 oct. 2018.

WANG, L.; RANJAN, R. (2015). “Processing distributed Internet of Things data in clouds.” IEEE Cloud Computing, vol. 2, n. 1, p. 76-80. Disponível em: https://ieeexplore.ieee.org/document/7091808/. Acesso em: 13 jun. 2018.

WEF (2018). “The global risks report 2018”. World Economic Forum. Disponível em: http://wef.ch/risks2018. Acesso em: 6 de ago. 2018.

ZANNI, A. (2015). “Sistemas ciber-físicos e cidades inteligentes”. IBM. Disponível em: https://www.ibm.com/developerworks/br/library/ba-cyber-physical-systems-and-smart-cities-iot/index.html. Acesso em: 10 jun. 2018.

ZUCKERMAN, E. (2005). “How to blog anonymously. In: Handbook for bloggers and cyber-dissidents”. Reporters without Borders. Disponível em: https://archive.org/stream/media_Handbook-for-Bloggers-and-Cyber-Dissidents/Handbook-for-Bloggers-and-Cyber-Dissidents#page/n0. Acesso em 13 ago. 2018.

Sobre a série "Segurança Cibernética e Liberdades Digitais"

A série de artigos estratégicos integra o projeto *Segurança Cibernética e Liberdades Digitais* do Instituto Igarapé. Esta reúne um conjunto de artigos e notas estratégicas que visam proporcionar uma reflexão crítica sobre os principais desafios que permeiam a relação entre segurança, privacidade e o emprego de novas tecnologias no Brasil. As notas estratégicas foram desenvolvidas pela equipe com base em uma série de diálogos organizados entre 2017 e 2018 com representantes do setor privado, governo, sociedade civil, comunidade técnica e academia. Visando abarcar diferentes leituras e perspectivas sobre o balanço entre abordagens criminalizantes e o fortalecimento de direitos (tal como o direito à privacidade), a série também conta com artigos de especialistas para analisar o pós-Marco Civil à luz dos desafios supracitados.

Outras publicações do Instituto Igarapé

ARTIGOS ESTRATÉGICOS

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 latino-americano: 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 - 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
(Maio 2017)

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 das mulheres na linha de frente das forças armadas
Renata Avelar Giannini, Maiara Folly, 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
(Maio 2017)

ARTIGO ESTRATÉGICO 25 - Brazil, the internet and the Digital Bill of Rights Reviewing the state of Brazilian internet governance
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 Latin America
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 and Alison Joersz
(Junho 2017)

NOTA ESTRATÉGICA 25 - O futuro das operações de manutenção da paz das Nações Unidas: uma perspectiva brasileira (implementação do relatório HIPPO)
Eduarda Hamann e 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 2359-0998

INSTITUTO IGARAPÉ

a think and do tank

www.igarape.org.br