lavits ****** 2017
5to Simposio Internacional LAVITS
Vigilancia, Democracia y Privacidad
en América Latina: Vulnerabilidades y resistencias

ISSN 2175-9596

SENSIBILIDADE PERFORMATIVA E PRIVACIDADE NA INTERNET DAS COISAS

Sensibilidad performativa y privacidad en Internet de las cosas

Performative Sensitivity and Privacy in the Internet of Things

Daniel Marques[a]
André Lemos[b]

[(a)] André Lemos é Professor Titular da Faculdade de Comunicação da Universidade Federal da Bahia. Pesquisador do CNPq.
[(b)] Daniel Marques é Professor Assistente do Centro de Cultura, Linguagens e Tecnologias Aplicadas (CECULT) da Universidade Federal do Recôncavo da Bahia. Doutorando em Comunicação (FACOM/UFBA).

Resumo

As relações entre privacidade, tecnologia e comunicação apresentam questões de alta relevância para os estudos em cultura digital. O presente artigo busca contribuir com o campo a partir de uma observação crítica dos problemas de privacidade na Internet das Coisas (IoT). Para tanto, desenvolvemos uma breve revisão sobre os principais aspectos da IoT e da privacidade, discutindo três casos – Google Home, Amazon Echo e Nest – a partir da abordagem teórica engendrada pelo conceito de Sensibilidade Performativa (SP) enquanto um operador teórico-metodológico importante para entender as múltiplas dimensões da privacidade na cultura digital, particularmente as que emergem com a IoT.
Palavras Chave: Sensibilidade performativa; Internet das coisas; Privacidade.

Abstract

The relations between privacy, technology and communication present issues of high relevance for studies in digital culture. The present article seeks to contribute to the field based on a critical observation of the problems of privacy in the Internet of Things (IoT). To do so, we developed a brief review of the main aspects of IoT and privacy, discussing three cases - Google Home, Amazon Echo and Nest - from the theoretical approach engendered by the concept of Performative Sensibility (PS) as an important theoretical-methodological operator to understand the multiple dimensions of privacy in digital culture, particularly those emerging with IoT.

Keywords: *Performative sensibility; Internet of things; Privacy.*

Resumen

Las relaciones entre privacidad, tecnología y comunicación presentan cuestiones de alta relevancia para los estudios en cultura digital. El presente artículo busca contribuir con el campo a partir de una observación crítica de los problemas de privacidad en Internet de las Cosas (IoT). Para ello, desarrollamos una breve revisión sobre los principales aspectos de la IoT y de la privacidad, discutiendo tres casos - un enfoque teórico engendrado por el concepto de Sensibilidad Performativa (SP) como un operador teórico-metodológico importante para entender las múltiples dimensiones de la privacidad en la cultura digital, particularmente las que emergen con la IoT.
Palabras Clave: *Sensibilidad performativa; Internet de las cosas; Intimidad.*

INTRODUÇÃO

O presente trabalho toma como objetivo central problematizar a questão da privacidade no contexto da Internet das Coisas, tomando como operador teórico-metodológico o conceito de sensibilidade performativa (SP) (Lemos & Bitencourt, 2017). Investigar a privacidade na IoT requer a observação de uma ampla rede composta pela agência de múltiplos atores: desde o sensor embarcado no produto IoT até o discurso corporativo das empresas que comercializam os objetos. O artigo apresenta uma discussão teórica-conceitual acerca da IoT, da sensibilidade performativa e da privacidade, trazendo a luz as questões que serão observadas com maior detalhe nos casos analisados. Pretendemos demonstrar, a partir de alguns casos – Google Home, Amazon Echo e Nest –, como as ameaças à privacidade surgem a partir da SP da IoT. Por fim, apontaremos algumas ações que podem minimizar os problemas identificados.

INTERNET DAS COISAS

A Internet das Coisas (IoT – *Internet of Things*) é uma rede na qual objetos físicos são instrumentalizados com sensores e ganham capacidades infocomunicacionais. A partir de procedimentalidade algorítmica independente de uma ação direta *human-to-human* ou *human-to-computer* (Gonzales & Djurica, 2015 citado em Martin, 2015), esses objetos tomam decisões relacionadas ao contexto, trocam informações, reconhecem identidades e desencadeiam ações em uma ampla rede.

O crescimento da IoT é global e acelerado. De acordo com estimativas da McKinsey Global Institute, a IoT poderá gerar um impacto econômico de US$ 11 trilhões até 2025. Em 2008, já havia mais objetos conectados à Internet do que pessoas. Estudos preveem que até 2020 esse número vai atingir 50 bilhões de objetos. No entanto, a maioria das pessoas (87%) nunca ouviu falar do assunto (Sowe, Kimata, Dong, & Zettsu, 2014). A narrativa da IoT afirma que com objetos inteligentes as cidades serão mais administráveis, resilientes e sustentáveis, os corpos serão mais saudáveis, os processos industriais serão mais produtivos, a gestão, o controle, o monitoramento e a vigilância de pessoas, informações e objetos serão mais eficientes etc. A IoT é uma ampla rede de agência entre objetos tendo como base a troca de dados entre os objetos, entre as empresas, acesso a banco de dados, criação de discursos científicos, publicitários, tecnocráticos que sustentam a necessidade de uso desses objetos.

O mercado da IoT é um dos grandes impulsionadores do que Silveira (2017a) chama de biopolítica da modulação de comportamentos, baseada na microeconomia da interceptação de dados, na intrusão de dispositivos de rastreamento e do direito à privacidade como a conhecemos. Essa nova economia informacional, pautada na comercialização de dados pessoais, requer a desarticulação das garantias individuais de privacidade conforme estabelecidas nas democracias modernas (Silveira, 2017b). Torna-se necessário ir além do núcleo do objeto para entender os desafios gerais da IoT e os que remetem ao nosso tema, a privacidade.

Múltiplos problemas de privacidade (bem como segurança e vigilância) surgem: desde a definição do tipo de dado captado pelos sensores, passando por suas formas de circulação e armazenamento, pelo compartilhamento com empresas parceira, pela relação com outros dados em banco de dados, pela interface de configuração de preferências pessoais etc. Casos recentes[1] mostram a vulnerabilidade da IoT, além de reforçar a necessidade se discutir sobre o controle – ou falta de controle – que os indivíduos possuem sobre a circulação de informações sobre si. A partir do momento em que os dados pessoais são dataficados em tempo real, integrando uma rede ampla e espraiada através da SP, o seu controle sobre a vida privada é constantemente desafiado pelos outros participantes da rede.

[1] Problemas com os dispositivos inteligentes da Samsung, o termostato Nest da Google, o dispositivo doméstico da Amazon, Amazon Echo e o vírus Mirai, entre outros. Ver https://www.theverge.com/2016/5/2/11540246/samsung-smart-things-security-study-critical-flaw-apps, https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#6a886f833986, http://www.independent.co.uk/news/world/americas/amazon-echo-murder-investigation-data-police-a7621261.html e https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

SENSIBILIDADE PERFORMATIVA

A IoT é uma rede de objetos dotados de sensibilidade performativa. Como discutido em textos anteriores (Lemos, 2016; Lemos & Bitencourt, 2017), compreendemos a SP enquanto uma forma específica de produção de performances e sensibilidades advinda dos fenômenos de "dataficação" (Mayer-Schönberger; Cukier, 2013; Van Dijck 2014; Kennedy, Poell, & Dijck, 2015). A sensibilidade e performatividade de seus objetos são produzidas em grande parte pelos algoritmos que os constituem, e nesse sentido é procedimental, digital, e distribuída em rede (Bogost, 2007; Bogost, 2008; Manovich, 2013). Podemos compreender esses objetos como *sencientes*, capazes de perceber a si mesmos e o ambiente, comunicando-se de forma autônoma em uma rede digital, gerando mediações (agências) em outros objetos, instituições e/ou humanos:

> Como a diversidade de objetos da IoT é crescente (os exemplos variam de acessórios de vestir até medicamentos – *ingestibles*), a SP afetará diversos aspectos da cultura contemporânea. Os reflexos alcançam diversas áreas da vida social com implicações amplas, já reconhecidas, inclusive, pela Federal Communications Commission (FCC, 2016). A SP é essa qualidade de um objeto-rede (Lemos & Bitencourt, 2017, p. 7).

A privacidade protegida e embarcada, ou as ameaças a ela, são consequências da SP nos projetos de IoT. Ao analisar um caso, podemos identificar como sua rede que se constitui e como as mediações atuam no sentido de proteger ou ameaçar a privacidade. Por exemplo, uma lâmpada que detecta movimentos, mas não identifica a face nem cruza esses dados desse usuário com outros bancos de dados têm uma SP construída para a proteção da pessoa. Há, nesse caso, uma intencionalidade no projeto do produto em preservar a impessoalidade do dado.

A SP é uma propriedade "sensorializada[2]" (Smith, 2016) que se reflete em uma rede de objetos produzindo ações (atuadores) e narrativas (discursos, ideologias) contextualizadas e personalizadas com base nas estratégias de circulação, compartilhamento, processamento e análise agregada de múltiplas bases de dados. A SP dos objetos da IoT vai muito além do objeto (do sensor, da conexão com a internet, da ação de algoritmos, dos atuadores isoladamente) e torna-se um "dispositivo"

[2] Smith (2016) se refere tanto ao fenômeno de sensores embarcados que extraem dados e agem sobre objetos mundanos quanto aos reflexos da agência desses dispositivos.

(Foucault, 2015) sofrendo e produzindo agências proveniente de *feedbacks* formatados pela procedimentalidade dos sistemas informáticos que passam a integrar a materialidade desses objetos. A SP é um ator-rede (Latour, 2005; Lemos, 2013).

PRIVACIDADE E IOT

A garantia da privacidade é um dos pilares da sociedade moderna e do estado de direito. Ela é indispensável para a manutenção de sociedades democráticas. Pode-se defini-la como um direito de controle, por parte do indivíduo, sobre a circulação das suas informações pessoais, um direito de ser deixado em paz, de não ter seus dados registrados ou usados por terceiros. O conceito remete à preservação da integridade do corpo, a limitação do acesso a determinados territórios e a dados e informações sobre uma pessoa. Consequentemente, há uma forte relação entre o entendimento de privacidade e a proliferação de objetos técnicos.

Formatos comunicacionais tensionam esse conceito, já que privacidade diz respeito também a restrição do acesso a informações por diversos meios de comunicação. Warren e Brandeis (1890) mostram como o surgimento da fotografia instantânea e a massificação do jornalismo impresso agiram como "invasores" produzindo "riscos" para o ambiente sagrado da vida privada doméstica.

Os fenômenos de midiatização (Hepp, 2013) ao longo da história reconfiguram esse campo. Na atual sociedade da informação, o conceito está ligado à habilidade de uma pessoa em controlar a exposição e a disponibilidade de dados acerca de si (Vianna, 2006). A ITU (2015) destaca que a cinco dimensões da privacidade (controlar informações sobre si mesmas; protege contra incômodos indesejados; é o direito de ser deixada sozinha; é obrigação recíproca de divulgação entre as partes; é um agente regulador visando equilibrar a coleta de dados).

No âmbito da IoT a questão é central (O'Hara, 2015). A IoT combina dispositivos pequenos, baratos e em algumas áreas eles estarão em vigor por vários anos. Os dados que eles movimentam são de difícil rastreamento e devem ser protegidos de intercepção. O consentimento de uso deve ser discutido. A IoT produz formas de comunicação e interação entre agentes, multiplicando as interfaces de acesso a informação e os métodos de comunicação. A possibilidade de compartilhar batimentos cardíacos a partir de dispositivos vestíveis, por exemplo, datafica cotidianamente novas categorias de informações

pessoais, transformando-as em dado que circulam em uma rede complexa, heterogênea e com interesses político-econômicos diversos. Ao longo da última década, com a proliferação de bens de consumo conectados a internet, o fenômeno ganhou expressividade mercadológica, política, legal e social, amplificando o número de estudos que se debruçam sobre o fenômeno e seus tensionamentos (Bunz, 2016; Christ & Winterthur, 2015; Karimova & Shirkhanbeik, 2015; Nansen, Ryn, Vetere, Robertson, Brereton, & Dourish, 2014).

Entendimentos sobre o que é e quais os limites da privacidade são contextuais e contingenciados por diversos campos da vida social e pelos entendimentos diferenciados dos sujeitos (Decew, 1997; Parker, 1973; Solove, 2002; Westin, 1984; Ponciano, Barbosa, Brasileiro, Brito, & Andrade, 2017). A diferença entre a percepção da gravidade do problema, e a forma como se comportam os indivíduos caracterizam o "paradoxo da privacidade". No caso dos sistemas informacionais, é comum o usuário se posicionar como preocupado em relação à circulação de suas informações pessoais e, ao mesmo tempo, sujeitar-se a utilidade de fazer parte do sistema e compartilhar dados para ter serviços em redes sociais digitais, por exemplo (Kehr, Kowatsch, Wentzel, & Fleisch, 2015; Kokolakis, 2017; Oetzel & Gonja, 2011; Wakefield, 2013).

Conceituar a privacidade não é simples. Historicamente o conceito de privacidade tem sido alvo de estudos das mais diversas naturezas e áreas do conhecimento como a filosofia, o direito, a sociologia, antropologia etc. São diversas correntes que produzem uma variedade de definições e abordagem (Solove, 2002; Kang, 1998; Decew, 1997). De uma forma genérica podemos dizer que privacidade é uma questão que remete à preservação da integridade do corpo, a limitação do acesso de terceiros a determinados espaços e territórios, ao acesso a dados e informações sobre uma pessoa. O campo da mídia e da comunicação é um tensionador do conceito, desde a formação da opinião pública com o jornalismo no começo do século XX, até as atuais polarizações público-privado com as redes sociais como Facebook. Certamente privacidade diz respeito a restrição do acesso a informações pessoais por comunicações, mensagens e/ou produtos midiáticos de terceiros – outros indivíduos ou instituições. Tanto os fenômenos de midiatização (Hepp, 2013) quanto o próprio aumento da presença de objetos IoT na vida cotidiana reconfiguram esses campos.

No que se refere à IoT podemos apontar quatro dimensões principais para enquadrar os problemas de privacidade (Ponciano et al., 2017):

1. a coleta indiscriminada de dados pessoais;
2. a inferência de novas informações através do cruzamento de dados e *machine learning*;
3. a troca e compartilhamento de informações com terceiros e;
4. a percepção de utilidade do produto em detrimento do risco de sua utilização – paradoxo da privacidade.

Nessas dimensões podemos apontar sete principais riscos à privacidade, sendo as três primeiras anteriores ao advento da IoT, mas amplificadas pela nova tecnologia, e as últimas particulares à IoT (Ziegeldorf, Morchon, & Wehrle, 2014; Aleisa & Renaud, 2017).

1. As possibilidades de identificação,
2. rastreamento,
3. perfilização,
4. ameaças de interações invasivas,
5. ciclo de vida obscuro,
6. ataques a inventário e
7. conexão a bases de dados de terceiros.

A partir de uma revisão sistemática de literatura de um total de 122 artigos sobre IoT e privacidade, utilizando como base as características definidas por Ziegeldorf et al. (2014), o rastreamento dos dados por terceiros aparece com uma das principais preocupações apontadas pela literatura (31.5%), principalmente no que diz respeito à localização do usuário. Destacam-se também compartilhamento de dados identificáveis com terceiros (26%) e perfilização (21%) enquanto ameaças significativas

COLETA DE DADOS PESSOAIS

Essa é uma possível entrada para a rede que vai se desenvolver com a SP. O sensor que está na base do objeto começa sua ação ao sentir uma grandeza física e transformá-la em dados que serão compartilhados com outros objetos. A escolha de que grandeza física sentida será transformada em dados, e como esses dados serão veiculados já coloca a SP no cerne do problema da privacidade.

Há um aumento quantitativo e qualitativo no que tange a coleta de dados pessoais (Ziegeldorf et al., 2014). Quantitativo, pois a escala de produtos conectados no cotidiano cresce exponencialmente, o que coloca o indivíduo enquanto fonte de dados – *data subject* – tanto para os bens que possui como para produtos de terceiros, uma possível Internet das Coisas dos Outros (Jones, 2015). A mudança qualitativa, por sua vez, diz respeito à crescente variedade de dados e informações pessoais que passam a ser quantificáveis e passíveis de coleta pelas tecnologias IoT – novos *data sets* fazendo com que a SP funcione de forma mais espraiada nesse contexto de coleta de dados, colocando em tensão e discussão o que se compreende enquanto público e privado.

A SP que configura esses objetos produz na extensão da sua rede novas possibilidades de coleta, análise e processamento de informações pessoais identificáveis (PII, *personally identifiable information)*. Essas são formas ampliadas de coleta, quantificação e processamento de informações pessoais criando publicação de dados que, outrora, seriam considerados estritamente privados. O dado captado entra em regime de circulação pois são compartilhados em *data centers*, servem para gerar prognósticos (Big Data) e fazem outros objetos agirem de acordo, ou vão criar discursos que serão publicados como "o espaço urbano ficará mais eficiente", "a casa será mais segura" ou o "usuário terá mais saúde". O discurso corporativo sobre a “morte da privacidade” enquanto um fenômeno natural e positivo para a sociedade contemporânea é parte da SP.

INFERÊNCIA DE NOVAS INFORMAÇÕES

A SP não se limita ao sensor ou atuador no objeto. Ela é um ator rede que desenvolve agência de amplo alcance. A informação captada pode ser utilizada em recombinações futuras (Kitchin, 2014). Grandes quantidades de dados não indexais são unidas e rastreados através de identificadores compartilhados, permitindo discriminação, combinação, desagregação e re-agregação, busca e outras formas de processamento e análise. Uma forma dessa ação se dá no processamento e na performance dos algoritmos (Finn, 2017).

Nesse sentido, os objetos da IoT poderiam produzir conclusões e inferências sobre o sujeito, sem que este tenha conhecimento, a partir das informações performadas pela SP desse objeto. Por exemplo, um dado sobre batimento cardíaco captado de um "relógio inteligente" pode, sendo cruzado com outros dados de outros sistemas, indicar passagens aéreas para determinados locais tirando proveito

do estado de tensão ou relaxamento em que se encontra o usuário. Ao utilizar um objeto que mede os batimentos cardíacos a primeira intenção do usuário é monitorar seu coração, mas a SP produz agências amplas sem que o usuário se dê conta. Na medida em que o espalhamento de objetos IoT se estende para o corpo, o lar, as práticas de consumo e a rotina dos sujeitos, os padrões e tornam-se mais visíveis aos algoritmos do que ao usuário.

Um dos discursos que podemos acoplar a SP da IoT é o da crescente fetichização dos algoritmos e dos sistemas computacionais nos produzir uma aura de confiabilidade. A SP ganha discursos científicos e racionais dos algoritmos, sendo construída assim para oferecer ao usuário interpretações neutras e precisas sobre a realidade vivida. Um dos efeitos colaterais é o que Danaher (2016) chama de "algocracia", tomada tecnocrática e burocrática dos algoritmos agindo de forma opaca e sem sem transparência para o usuário desses sistemas.

COMPARTILHAMENTO DE INFORMAÇÕES COM TERCEIROS

Uma das facetas da SP ampliar sua agência algorítmica para objetos e sistemas muito mais amplos, permitindo o acesso de dados pessoais por parte de empresas diretamente envolvidas, empresas parceiras destas (Buchenscheit, Könings, Neubert, Schaub, Schneider, & Kargl, 2014; Knijnenburg & Kobsa, n.d.) e governos (Ponciano et al., 2017) que podem fazer uso desses dados para gerar ações e efeitos de consequências diversas (comerciais, policiais, políticos). O sujeito deixa de ser o único receptor do dado coletado e processado – *data recipient* – e essas informações servirão para práticas diversas de perfilização – *profiling* – e identificação pessoal, produzindo novos tipos e estratégias de informação pessoal identificável.

Essa ação por processos em rede, opacos, pouco visíveis e compreensíveis, apontam para problematizar até que ponto o que Ziegeldorf et al. (2014) chamam de "autodeterminação informacional" (*informational self-determination), pode ser exercida com consciência. Essa determinação refere-se* à capacidade do sujeito em avaliar os riscos pessoais de privacidade, de agir em prol da sua proteção e de ter clareza de que suas decisões serão mantidas para além da sua esfera de controle imediato. Com a IoT não há clareza sobre a captura (ponto 01), a inferência de novos dados (ponto 02), nem sobre quais e como as informações são compartilhadas com terceiros (ponto 03).

A ideia de fronteiras de informação (*information boundaries)* como sugerida por Ponciano et al. (2017), é interessante, pois já subentende uma rede ampla de performances de dados. Essa noção confere a cada indivíduo a possibilidade de se engajar em um processo dinâmico de "abertura" e "fechamento" do acesso a suas informações pessoais, produzindo assim fronteiras fluidas que delimitarão o acesso aos dados. Além disso, cada sujeito poderá trabalhar em prol da definição de regras específicas que definirão o movimento dessas fronteiras. Essas regras, por sua vez, são ancoradas no cálculo de risco *versus* benefício – paradoxo da privacidade – em se engajar em determinada abertura e liberação de dados e informações pessoais.

Contudo, como apontamos e compreendermos a performance da SP, a delimitação das fronteiras de acesso – ou das esferas de controle – no cenário da IoT se torna muito mais complexa e por isso preferimos falar de politizar as performatividades das bordas entre objetos e sistemas. Em grande medida, graças ao regime de invisibilidade dos dispositivos e algoritmos coletores de dados: não há transparência total sobre o que pode estar sendo coletado e quando a coleta acontece. Ou seja, há uma indeterminação ou desconhecimento por parte do sujeito sobre em que situações ampliar ou reduzir suas fronteiras de acesso.

UTILIDADE *VERSUS* RISCO (PARADOXO DA PRIVACIDADE)

A utilidade de um objeto inteligente é uma das razões de ser de sua SP: captar dados do ambiente, retirar informações complementares e compartilhá-las, como vimos nos três aspectos anteriores. Quanto mais útil o produto aparenta ser, menores serão as preocupações do usuário com problemas de privacidade (Ponciano et al., 2017), reforçando o paradoxo da privacidade. Esse paradoxo varia de acordo com a experiência dos usuários, a usabilidade e o design dos dispositivos, a percepção de risco a privacidade, as normas sociais e os termos e normas de privacidade.

Williams, Nurse e Creese (2016), por exemplo, acreditam que com a IoT esse paradoxo será ampliado. Seu argumento toma como base aspectos específicos da SP, particularmente aqueles que se relacionam às interfaces dos produtos IoT, a ubiquidade da coleta de dados e a ação do mercado (Williams et al., 2016). Sobre as interfaces, entende-se que a heterogeneidade de produtos inteligentes e suas múltiplas interfaces produzem dificuldades no usuário médio em manipular os aparelhos.

A invisibilidade sobre a coleta e compartilhamento de dados é outro problema sério, visto que sem essa informação o usuário não pode sequer entender o que é feito com seus dados pessoais.

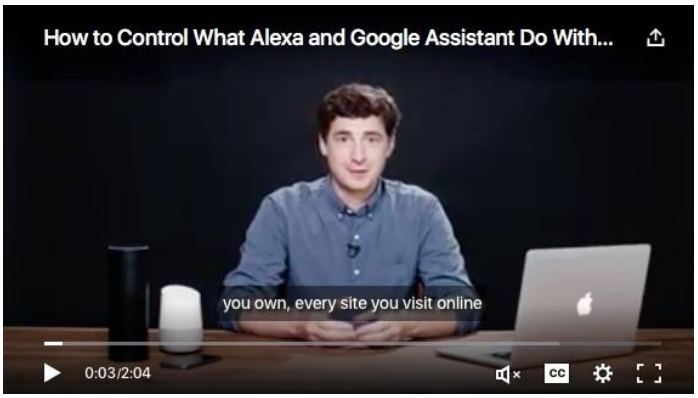
A dimensão mercadológica, que está embutida nessa rede sociotécnica que é a SP do objeto inteligente, contribui para o aprofundamento do paradoxo da privacidade. Isso ocorre por dois motivos. Em primeiro lugar, graças ao contínuo lançamento de produtos que para serem mais baratos e competitivos não investem muito em segurança ou em opções de configuração de privacidade. Embora estudos específicos apontem para metodologias e estratégias de projeto voltados à proteção dos dados do usuário – campo conhecido como *privacy by design*, privacidade pelo design ou privacidade projetada (Cavoukian & Jonas, 2012; Doty & Gupta, 2013; Lentzsch, Loser, Degeling, & Nolte, 2017) –, a necessidade de lançar produtos novos e mais baratos interfere na lógica da qualidade. Em segundo lugar, o modelo de negócio é pautado na comercialização, troca e análise de dados pessoais, principalmente para a indústria da publicidade e e-commerce. Os atuais fenômenos como a perfilização só são possíveis graças a essa lógica.

ESTUDOS DE CASO: GOOGLE HOME, AMAZON ECHO E NEST

Alguns exemplos recentes podem nos ajudar a ilustrar a questão da privacidade na rede da SP na IoT. Vídeo recente (Figura 1) mostra como reforçar a privacidade com o Google Home e o Amazon Echo. Esses dispositivos, quando ativados, enviam os dados de voz para as empresas a fim de fornecer a informação demandada. Mas, segundo informam, não escutam até que o usuário os ative ("Ok Google" ou "Alexa"), nem enviam informações nominais a terceiros. Mas tudo fica nos servidores até que o usuário apague as informações[3].

[3] https://www.wired.com/story/amazon-echo-and-google-home-voice-data-delete. Recuperado em 30 de outubro de 2017.

Figura 1



Daniel Marques e André Lemos: *Screenshot* - Interação com Alexa e Google Home sobre privacidade. 2017.

Mas há casos de intrusão. O caso recente envolvendo a Burger King e o *smart hub* Google Home[4] é um exemplo de interação invasiva (Ziegeldorf et al., 2014). Em um comercial televisivo de 15 segundos veiculado em abril desse ano nos Estados Unidos, o ator em cena – caracterizado como funcionário da lanchonete – argumenta que o tempo do vídeo é curto para apresentar de forma qualificada todos os ingredientes do Whopper, hambúrguer tradicional da rede. Assim, ele se aproxima da câmera e diz "Ok Google", ativando o Google Home na casa do espectador para realizar uma busca. E ele pede informações sobre o Whopper. Imediatamente o dispositivo é ativado e lê o verbete sobre o produto encontrado na Wikipedia (Figura 2). Embora não colha informações pessoais, essa ação configura-se como uma invasão de privacidade e uso de dispositivos pessoais à distância.

Figura 2

The New York Times: Interação do Comercial com Google Home. 2017.

[4] Ver https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html. Recuperado em 30 de outubro de 2017.

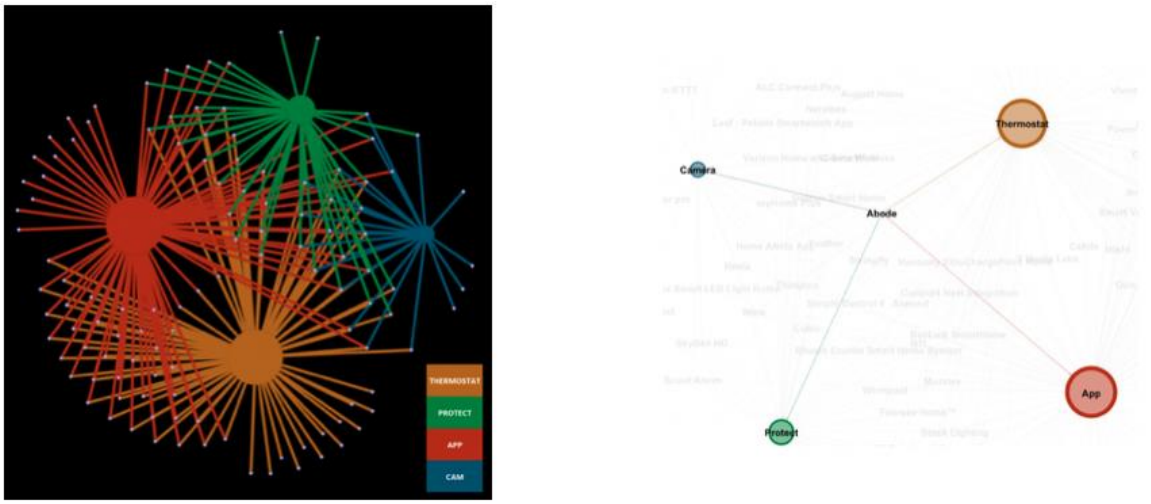
A interação do Google Home com o comercial materializa a vigilância constante do dispositivo que busca por *inputs* externos, e pode levantar dúvidas por parte do indivíduo sobre o que é seguro de se dizer na presença do aparelho. O discurso corporativo, na outra ponta da rede, reforça a neutralidade e obediência dos dispositivos, como o vídeo descrito na Figura 1 demonstra.

Outro exemplo interessante ocorreu em julho deste ano, dessa vez com o Amazon Echo, um dos smart *hubs* proprietários da Amazon. De acordo com a imprensa[5], a assistente pessoal Alexa – inteligência artificial embarcada no Amazon Echo – teria realizado um chamado de emergência para a polícia da cidade de Albuquerque, nos Estados Unidos, na ocasião de um ato de violência doméstica. Supostamente o aparelho teria agido de forma autônoma, ao interpretar a fala do agressor que ameaçava a vítima de morte caso "chamasse a polícia". Não se sabe exatamente como as forças polícias foram acionadas, tendo em vista que a realização da chamada requer, antes de tudo, a ativação do aparelho a partir de um comando específico (como o "Ok Google" no Google Home) e que aquele que receberá a ligação também tenha um Echo instalado. As perícias demonstraram posteriormente que é possível ouvir a vítima falando repetidamente "*call 911*", mas ainda não se sabe como o Echo foi ativado para interpretar o comando.

Para ilustrar a SP e a controvérsia da privacidade podemos montar a rede do termostato Nest, um dos mais populares objetos pessoais da IoT. Artigo recente de Dirkzwager, Cornelisse, Brok e Corcoran (2017) mostra os dados pessoais retirados do dispositivo e circulado entre parceiros (Figura 3). Esse exemplo confirma os quatro pontos centrais da privacidade em sua rede de SP (coleta de dados, inferências, compartilhamento e paradoxo da privacidade). A rede do termostato Nest (Figura 4) descreve a sensibilidade performativa em suas ações desde o usuário, o objeto, as formas de narrativas publicitárias, os dados compartilhados com empresas parceiras, a quantidade de dados trocados etc. Vemos como os sete problemas da privacidade apontados por Ziegeldorf et al. (2014) se posicionam na rede.

[5] Ver https://www.nytimes.com/2017/07/11/business/amazon-echo-911-emergency.html. Recuperado em 30 de outubro de 2017.

Figura 3



Aimee Dirkzwager, Jimi Cornelisse, Tom Brok e Liam Corcoran: Os mapeamentos mostram, a esquerda as diferentes conexões de dados compartilhados entre dispositivos, e a imagem da direita os dados sendo compartilhados com outros aplicativos. 2017.

Figura 4

Daniel Marque e André Lemos: Rede da SP do termostato NEST e sua relação com a questão da privacidade. 2017.

O usuário fornece dados de referência pessoal e o objeto estuda o horário deste usuário, aprendendo, por exemplo, a temperatura preferida para a casa. Usando sensores integrados e geotracking, o Nest passa para o modo de economia de energia quando ele compreende que o usuário não está em casa ou em locais específicos do ambiente. A empresa possui além do aplicativo e do termostato, outros objetos ("Protect" - detector de fumaça e monóxido de carbono; "Cam" com visão noturna, alertas de fala, som e movimento). O aplicativo permite o acesso a todos os dispositivos. A pesquisa mostra que há 116 parceiros que recebem dados da Nest, variando de câmeras de bebê a frigoríficos inteligentes e lâmpadas. Esses dispositivos rastreiam inúmeros dados dos usuários, incluindo métricas de uso do dispositivo, endereços IP, detalhes de contato, pagamentos e muito mais.

A rede expõe a SP e as questões de privacidade e IoT apontadas anteriormente. Descreve-se o objeto, a casa, as formas de narrativas publicitárias, os dados compartilhados com empresas parceiras e a quantidade de dados trocados. Podemos identificar os sete problemas da privacidade apontados anteriormente e como eles se posicionam na rede (1. Identificação, 2. Localização, 3. Geração de perfil, 4. Circulação publica de dados privados, 5. Transações no ciclo de vida do objeto, 6. Buscas de dados em outros inventários, 7. Combinação de dados em outros sistemas). Esse exemplo confirma os quatro pontos centrais da privacidade em sua rede de SP (coleta de dados, inferências, compartilhamento e paradoxo da privacidade).

CONCLUSÃO - SP COMO REDE E COMUNICAÇÃO DAS COISAS.

A questão da privacidade na IoT deve ser entendida de forma ampla, partindo do reconhecimento da SP como um princípio desses objetos e um ator-rede (Latour, 2005). A SP é um conjunto de ações, uma comunicação das coisas, que afeta o objeto em suas mais diversas dimensões: uso, interface, mercado, publicidade. Criptografar ou não os dados, integrar ou não esses dados com outros bancos de dados, promover ações de privacidade pelo design, compartilhar ou não dados, definir quais dados serão compartilhados, enquadrar discursos publicitários ou ações mercadológicas, a definição de quadros jurídicos, todas essas questões estão interligadas à performance algorítmica da SP desses objetos. Reforçando o entendimento de Solove (2002), a SP demonstra como as práticas de privacidade são efetivamente construídas por diferentes instâncias (a funcionalidade do objeto, a interface gráfica de comando, os dados que ele retira do ambiente e como, o modelo de negócio e o discurso publicitário para sua venda destaca a eficiência energética e a segurança da casa). A questão da privacidade está imersa nessa rede desenvolvida pela SP.

Compreender a questão da privacidade é destacar um olhar sobre essa rede em deslocamento. As soluções devem se dar nos aspectos jurídicos, em alternativas de privacidade pelo design e em uma politização (educação) tornando visíveis as ameaças envolvidas e forçados os padrões de segurança a serem adotados pelas indústrias. De acordo com Hoepman (2012), tratam-se de estratégias que por um lado tratam de diretrizes, leis e políticas regulatórias – *privacy-by-policy* – e por outro envolvem a arquitetura dos próprios sistemas – *privacy-by-architecture* –. Um produto orientado à proteção da privacidade do indivíduo – privacy by design –, portanto, precisa abarcar esses dois polos. A SP se

articula de forma fluida, orgânica e dinâmica entre ambos, já que é possível verificar sua agência tanto na lei que regula o tratamento de dados pessoais como na criptografia instaurada no sensor. Modelos de confiabilidade na comunicação das coisas devem ser, portanto, visualizados (*blockchain* para certificar que um objeto está mesmo falando a verdade para outro). Uma comunicação das coisas está em construção, com objetos buscando parceiros em uma espécie de rede social dos objetos (Karimova & Shirkhanbeik, 2015), tornando ainda mais aguda a discussão sobre a privacidade.

Sintetizando, é possível dizer que:

1. A questão da privacidade é uma das dimensões a ser avaliadas em uma análise das performatividades dos objetos da IoT;
2. Algumas soluções devem ser enquadradas em um sistema legal;
3. Práticas de privacidade por design – embarcadas no projeto dos produtos – devem ser desenvolvidas;
4. Redes federadas e/ou blockchains podem ser modelos de interessantes a serem desenvolvidos para dar confiabilidade na comunicação das coisas;
5. Desenvolver e melhorar os padrões de segurança a serem adotados pelas indústrias;
6. Desenvolver interfaces de configuração amigáveis nas quais os ajustes de privacidade sejam claros e transparentes;
7. Politização. Tornar visíveis as ameaças envolvendo parceiros e gerenciamento de dados.
8. Compreender a vida social dos objetos. Uma comunicação das coisas está em construção. Os objetos poderão encontrar parceiros em uma espécie de rede social de objetos, ampliando as ameaças à privacidade e invisibilidade dos algoritmos.

REFERÊNCIAS

Aleisa, N., & Renaud, K. (2017). *Privacy of the Internet of Things:* A Systematic Literature Review. Proceedings of the 50th Hawaii International Conference on System Sciences, 5947–5956.

Brandreis, L. D., & Warren, S. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193–220.

Buchenscheit, A., Könings, B., Neubert, A., Schaub, F., Schneider, M., & Kargl, F. (2014, dezembro). *Privacy implications of presence sharing in mobile messaging applications*. Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia - MUM '14, 20–29.

Bunz, M. (2016). The Internet of Things: tracing a new field of enquiry. *Media, Culture & Society*, 2016.

Cavoukian, A. & Jonas, J. (2012, junho 08). Privacy by Design in the Age of Big Data. *Information and Privacy Commissioner of Ontario* [p. 17].

Christ, O., & Winterthur, L. (2015). Martin Heidegger's Notions of World and Technology in the Internet of Things age. *Asian Journal of Computer and Information Systems, 3*(2), 58–64.

Danaher, J. (2016). The Threat of Algocracy: Reality, Resistance and Accommodation. *Philosophy and Technology, 29*(3), 245–268.

Decew, J. W. (1997). *In pursuit of privacy : law, ethics, and the rise of technology* [s.l.]. Ithaca: Cornell University Press.

Dirkzwager, A., Cornelisse, J., Brok, T, & Corcoran, L. (2017, outubro). Where does your data go? Mapping the data flow of Nest. *Masters of Media*. Recuperado em 30 de outubro de 2017 de https://mastersofmedia.hum.uva.nl/blog/2017/10/25/where-does-your-data-go-mapping-the-data-flow-of-nest.

Doty, N., & Gupta, M. (2013). *Privacy Design Patterns and Anti-Patterns Patterns Misapplied and Unintended Consequences*. Proceedings of the Ninth Symposium on Usable Privacy and Security. Recuperado em 30 de outubro de 2017 de https://cups.cs.cmu.edu/soups/2013/trustbusters2013/Privacy_Design_PatternsAntipatterns_Doty.pdf.

Finn, E. (2017). *What Algorithms Want: Imagination in the Age of Computing* [s. l., s. n.].

Foucault, M. (2015). *Microfísica do poder* [2. ed.]. Rio de Janeiro: Paz e Terra.

Hepp, A. (2013, dezembro). The communicative figurations of mediatized worlds: Mediatization research in times of the "mediation of everything". *European Journal of Communication, 28*(6), 615–629.

ITU (2015). *Privacy and Ubiquitous Network Societies* [Background Paper]. ITU.

Jones, M. L. (2015). Privacy Without Screens & The Internet of Other People's Things. *Idaho Law Review, v. 51*, 639–660.

Karimova, G. Z., & Shirkhanbeik, A. (2015). Society of things: An alternative vision of Internet of things. *Cogent Social Sciences*, *1*(1), 1–7.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635.

Kennedy, H., Poell, T., & Dijck, J. van (2015). Data and agency. *Big Data & Society, 2*(2), 1-7. Recuperado em 30 de outubro de 2017 de http://bds.sagepub.com/lookup/doi/10.1177/2053951715621569.

Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. Londres: Sage.

Knijnenburg, B., & Kobsa, A. (n.d.). Increasing Sharing Tendency Without Reducing Satisfaction: Finding the Best Privacy-settings user interface for social networks. *Thirty Fifth International Conference on Information Systems*, 1–21.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security, v. 64*, 122–134.

Latour, B. (2005). *Reassembling the Social:* An Introduction to Actor-Network Theory. Oxford: Oxford University Press.

Lemos, A., & Bitencourt, E. (2017, junho). Sensibilidade Performativa e Comunicação das Coisas: Explorando as narrativas algorítmicas na Fitbit Charge HR2. *Anais do XXVI Encontro Anual da Compós*, Faculdade Casper Líbero, São Paulo, SP.

Lemos, A. (2016). Sensibilités Performatives. Les nouvelles sensibilités des objets dans les métropoles contemporaines. *Revue Sociétés, 132*(2), 71-84.

Lentzsch, C., Loser, K., Degeling, M., & Nolte, A. (2017). Integrating a Practice Perspective to Privacy by Design. In T. Tryfonas (Ed.). *Lecture Notes in Computer Science*. Cham: Springer International Publishing.

Manovich, L. (2013). *Software takes command*. Nova Iorque: Bloomsburry Academic, 2013.

Martin, R. (2015, dezembro 28). The Internet of Things (IoT) – Removing the Human Element. *Infosec Writers*. Recuperado em 5 de maio de 2016 de http://www.infosecwriters.com/Papers/RMartin_IoT.pdf.

Nansen, B., Ryn, L. van, Vetere, F., Robertson, T., Brereton, M., & Dourish, P. (2014). An internet of social things. *Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures the Future of Design* - OzCHI'14, 87–96.

Oetzel, M. C., & Gonja, T. (2011). *The Online Privacy Paradox:* A Social Representations Perspective. Chi 2011, 2107–2112.

Parker, R. B. (1973). A Definition of Privacy. *Rutgers Law Review, v. 27*.

Ponciano, L., Barbosa, P., Brasileiro, F., Brito, A., & Andrade, N. (2017, agosto). Designing for Pragmatists and Fundamentalists: Privacy Concerns and Attitudes on the Internet of Things. *Brazilian Symposium on Human Factors in Computing Systems* (HC'17), 2017, Joinville, SC, Brasil.

Silveira, S. A. da (2017a). Governo dos algoritmos. *Revista de Políticas Públicas, 21*(1), 267, 2017a.

Silveira, S. A. da (2017b). *Tudo sobre tod@s:* Redes digitais, privacidade e venda de dados pessoais [1. ed.]. São Paulo: Edições Sesc SP.

Solove, D. J. (2002, julho). Conceptualizing privacy. *California Law Review, 90*(4), 1087-1155. Recuperado em 30 de outubro de 2017 de http://www.jstor.org/stable/3481326?origin=crossref.

Sowe, S. K., Kimata, T., Dong, M., & Zettsu, K. (2014). Managing Heterogeneous Sensor Data on a Big Data Platform: IoT Services for Data-Intensive Science. *Preecedings of the IEEE 38th Int. Comput. Softw. Appl. Conf. Work.*, 295–300.

Dijck, J. van (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance and Society, 12*(2).

Vianna, T. (2006). *Transparência pública, opacidade privada*. Tese de Doutorado em Direito, Universidade Federal do Paraná, Curitiba, PR, BR. Recuperado em 30 de outubro de 2017 de http://acervodigital.ufpr.br/bitstream/handle/1884/5281/VIANNA,%20TÃºlio%20Lima%20-%20Tese%20doutorado%20em%20Direito%20UFPR.pdf?sequence=1.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *Journal of Strategic Information Systems, 22*(2), 157–174.

Westin, A. (1984). *The origins of modern claims to privacy*. Cambridge: Cambridge University Press.

Williams, M., Nurse, J. R. C., & Creese, S. (2016). The Perfect Storm: The Privacy Paradox and the Internet-of-Things. *Proceedings of 2016 11Th International Conference on Availability, Reliability and Security* (Ares 2016), 644–652.

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the internet of things: Threats and challenges. *Security and Communication Networks*, *7*(12), 2728–2742.