ID 1611
Recebido em: 03/07/2018 | Aceito em: 24/06/2019

www.e-compos.org.br
| E-ISSN 1808-2599 |

Privacidade e Internet das Coisas: uma análise da rede Nest a partir da Sensibilidade Performativa

André Lemos
Universidade Federal da Bahia – UFBA, Salvador, Bahia, Brasil

Daniel Marques
Universidade Federal do Recôncavo da Bahia – UFRB, Santo Amaro, Bahia, Brasil
Universidade Federal da Bahia – UFBA, Salvador, Bahia, Brasil

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. Para tanto, desenvolvemos uma breve revisão sobre os principais aspectos da Internet das Coisas e da privacidade. O conceito de Sensibilidade Performativa será o operador teórico-metodológico criado e utilizado para entender as múltiplas dimensões do fenômeno. Como exemplo, é feita uma rápida análise do termostato Nest.

Palavras-chave
Sensibilidade Performativa. Internet das Coisas. Privacidade. Nest.

Introdução

Este artigo tem como objetivo problematizar a questão da privacidade no contexto da Internet das Coisas (IoT)[1], utilizando como operador teórico-metodológico o conceito de Sensibilidade Performativa (SP) (LEMOS, 2016; LEMOS; BITENCOURT, 2017). A questão da privacidade é central no desenvolvimento da cultura digital na contemporaneidade – marcada por sistemas algorítmicos digitais altamente performativos. Compreendê-la é examinar uma ampla rede composta pela agência de múltiplos elementos: desde o sensor embarcado nos objetos até o discurso corporativo técnico ou mercadológico. Há uma multiplicidade de forças que atuam no sentido de tensionar as fronteiras entre o público e o privado,

1 A "Internet das Coisas" (IoT – Internet ofThings) 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 *apud* MARTIN, 2015), esses objetos tomam decisões relacionadas ao contexto, trocam informações, reconhecem identidades e desencadeiam ações em uma ampla rede.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

revelando dimensões jurídicas, técnicas, sociais, culturais, midiáticas. Argumentaremos, ao longo do texto, que o rastreamento da rede através da SP nos auxilia na compreensão do fenômeno.

Mais do que na era da internet da Web 1.0 ou 2.0 (O'REILLY, 2005), a Internet das Coisas (IoT) é uma rede de objetos relativamente autônomos cujas ações interferem diretamente nos espaços públicos, no lar ou no corpo, seja com os atuais projetos de cidades inteligentes (*smart cities*), casas inteligentes (*smart home*), ou objetos vestíveis (*wearables*). Desde a definição do tipo de dado captado pelos sensores, passando por suas formas de circulação e armazenamento, pelo compartilhamento com empresas parceiras, pela relação com outros dados em bancos de dados e pela interface de configuração de preferências pessoais, as ameaças à vida privada circulam. Tomaremos como momento central e princípio da IoT a "sensibilidade performativa" dos objetos, como explicaremos a seguir. Ela dispara uma série de ações em uma ampla rede. Assim sendo, torna-se necessário ir além do núcleo do objeto para entender os desafios gerais que a IoT impõe à prática e ao entendimento sobre a privacidade.

A partir do momento em que pessoas, hábitos e espaços são "dataficados" (traduzidos por dados digitais e processamento algorítmico) (DOURISH; GÓMEZ CRUZ, 2018; MAYER-SCHÖNBERGER; CUKIER, 2013; SADOWSKI, 2019), integrando uma rede espraiada, o controle sobre a vida privada é constantemente desafiado. O mercado da IoT é, por exemplo, um dos grandes impulsionadores do que Silveira (2017b, p. 101) chama de "biopolítica da modulação de comportamentos", baseada na microeconomia da interceptação de dados, na intrusão de dispositivos de rastreamento e na ameaça ao direito à privacidade. Essa nova economia informacional, pautada na comercialização de dados pessoais e em um amplo processo de plataformização da sociedade (DIJCK; POELL; WAAL, 2018; SRNICEK, 2017) requer a desarticulação das garantias individuais de privacidade conforme estabelecidas nas democracias modernas. Esse cenário é complexo e, como aponta Silveira (2017b, p. 888), constitui um "ecossistema envolvendo um conjunto de actantes, empresas, plataformas, usuários, agências, data centers, programas de rastreamento, banco de dados, entre outros dispositivos".

É possível ver traços desse contexto em caso recente envolvendo a Burger King e o *smart*

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

speaker Google Home[2]. Em um comercial televisivo de 15 segundos, veiculado em 2017 nos Estados Unidos, um funcionário da lanchonete argumenta que o tempo do vídeo é curto para apresentar todos os ingredientes do Whopper, hambúrguer tradicional da rede. Em seguida ele se aproxima da câmera e diz: "Ok Google", ativando o Google Home na casa do espectador, pedindo para ele realizar a busca sobre o produto. O dispositivo entra em funcionamento e lê o verbete na Wikipedia. Vemos aqui uma forma de interação invasiva (ZIEGELDORF et al., 2014), mesmo não coletando informações pessoais. A "SP" e informacional do Google Home é acionada por alguém à distância, funcionando como um gatilho que vai mobilizar uma rede de ações colocando em xeque o controle do espaço privado da casa[3]. A agência algorítmica do dispositivo começa a se deslocar por uma ampla rede fugindo do controle do sujeito.

Não analisaremos os perigos da privacidade em casos de falhas de segurança ou *hacking* dos sistemas[4], mas os problemas que emergem do uso corriqueiro desses novos dispositivos, como ilustrado no comercial. A surpresa dos usuários frente a esse caso[5] revela que há um amplo desconhecimento sobre as questões ligadas à privacidade. Parte da dificuldade em identificar as ameaças vem da invisibilidade (PASQUALE, 2015) e da opacidade da agência em rede do sistema (cuja amplitude é difícil de discernir). O caso Burger King/Google Home, portanto, ajuda a reforçar a necessidade do escrutínio sobre a privacidade e a IoT.

A seguir apresentamos uma discussão teórica-conceitual acerca da sensibilidade performativa e das questões de privacidade referentes à IoT. Fazemos referência ao trabalho de Ponciano et al. (2017) para discutir os maiores desafios da privacidade no contexto da IoT: a) coleta indiscriminada de dados pessoais; b) inferência de novas informações; c) compartilhamento de informações pessoais com empresas parceiras; d) utilidade do uso *versus* risco: o paradoxo da privacidade. Para materializar a discussão, analisaremos a rede em

2 Disponível em: <https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html>. Acesso em: 03/07/2018.

3 Essa demanda poderá gerar, mais adiante, perfis sobre uso e consumo da informação desse usuário (nesse caso, de uma informação falsa, já que o sistema vai interpretar que a demanda é do morador).

4 Como ataques de tipo "Ramsonware", como os do malware Mirai que paralisou e sequestrou diversos sistemas ao redor do mundo em outubro de 2016.

5 Para mais informações, acesse: <theverge.com/2017/4/12/15259400/burger-king-google-home-ad-wikipedia>.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

torno de produtos da marca Nest, tomando como foco central o termostato, principal objeto inteligente do portfólio da marca.

A sensibilidade performativa na Internet das Coisas

Compreendemos a SP (LEMOS, 2016; LEMOS; BITENCOURT, 2017) enquanto uma forma específica de produção de performances e sensibilidades advinda dos fenômenos de produção, coleta e interpretação de dados e informações retiradas dos objetos e do ambiente (MAYER-SCHÖNBERGER; CUKIER, 2013; VAN DIJCK, 2014; KENNEDY; POELL; VAN DIJCK, 2015). A IoT é uma rede de objetos dotados de sensibilidade digital e de performatividade algorítmica. Acreditamos que essa é a particularidade da IoT. Ela é parte constitutiva da rede de objetos inteligentes que a define. Para entender a sua ação, podemos começar por qualquer ponto da rede, seja pelo discurso publicitário, as especificações técnicas, o uso quotidiano, os sensores embutidos nos objetos, a captação e troca de dados entre empresas etc. Seguindo sua ação é possível discutir diversos aspectos da IoT, como as questões de privacidade que descreveremos a seguir na rede Nest.

A SP é constituída do binômio "sensibilidade" e "performatividade". Por sensibilidade entendemos a capacidade dos objetos da IoT em sentir dados de outros objetos e do ambiente, transformando-os em procedimentos infocomunicationais, fazendo com que troquem informações e executem tarefas (BOGOST, 2007, 2008; MANOVICH, 2013, SMITH, 2016). Isso cria uma nova dimensão dos objetos quotidianos que passam a ser "ampliados" digitalmente.

Por performatividade entendemos a ampla agência (de dados, algorítmica) em que objetos executam (performam) em uma ampla rede. Ela tem a particularidade de seguir uma lógica algorítmica, não sendo circunscrita ao aspecto técnico. Ela desenvolve-se como um "fazer-fazer" em diversas instâncias: dimensões políticas, publicitária, econômicas, culturais etc. A SP projeta-se em uma rede realizando ações 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 constitui a IoT como um "ator-rede" (LATOUR, 2015, 2012), gerando um conjunto de ações. Algumas podem afetar diretamente a privacidade. Portanto, 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), tornando-se um "dispositivo", no

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

sentido foucaultiano do termo (FOUCAULT, 2015, p. 364-365)[6].

A privacidade protegida e embarcada – ou as ameaças a ela – são consequências da agência da SP nos projetos de IoT. Ao analisar um caso qualquer, podemos identificar como a rede da SP se constitui e como suas mediações atuam no sentido de proteger, ou ameaçar a privacidade. Por exemplo, uma lâmpada inteligente que detecta movimentos, mas não identifica nominalmente o usuário, nem cruza os seus dados com outros bancos de dados, teria uma SP constituída no sentido de aumentar a proteção da privacidade. Haveria, portanto, nesse caso, uma intencionalidade no projeto do produto cujo intuito seria preservar a não indexação do dado a um indivíduo. Se assim fosse, a operação "dividual" (DELEUZE, 1999) gerada pelo sistema (criação de perfil, duplos digitais, previsões sobre comportamentos etc.) não conseguiria remontar nominalmente à pessoa da qual foi extraída a informação. A SP gerencia a representação do dado entre um padrão dividual, que identifica perfis, e um conjunto de informações que, por não se referirem a um indivíduo em particular, são garantidas como privadas. Esse "dividuo", portanto, é constantemente produzido e reproduzido a partir dos aparatos de coleta e de processamento de dados pessoais, adicionando uma camada maior de complexidade à discussão sobre privacidade na IoT. A SP nos ajuda a localizar e problematizar múltiplas instâncias nas quais se materializa essa "privacidade dividual" (CHENEY-LIPPOLD, 2017), pois revela as "mediações radicais" (GRUSIN, 2015) atuantes na rede.

Sobre o conceito de privacidade

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[7]. Pode-se defini-la como

6 É importante salientar que todo objeto tem uma "sensibilidade" e desempenham "agências" (ou performatividades), que eles fazem-fazer em uma rede sociotécnica. No entanto, aqui nos referimos a uma sensibilidade e a uma performatividade específicas, cuja natureza central é a sua reação ao ambiente e ação sobre outros objetos de forma digital e algorítmica. Não temos espaço para desenvolver esse argumento neste artigo. Remetemos essa discussão para as obras de Graham Harman (2011), Bruno Latour (2005) ou Karen Barad (2007), entre outros, aliados à Ontologia Orientada à Objetos ou às sociologias pragmáticas como a Teoria Ator-Rede.

7 No caso do Brasil, o artigo 5 da Constituição (1988), assegura: X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. Cabe destacar também o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPDP), Lei nº 13.709/2018.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

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 historicamente à preservação da integridade do corpo, à 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 tensão criada pela a agência dos objetos técnicos na constituição do social.

Warren e Brandeis (1890), em seu artigo seminal *The Right to Privacy*, publicado há mais de um século, já destacavam as "ameaças" que o desenvolvimento tecnológico poderia engendrar. Os autores apontam diretamente para o surgimento da fotografia e a massificação do jornalismo impresso enquanto invasores ou potenciais riscos para o ambiente sagrado da vida privada doméstica. Desde a formação da opinião pública com o jornalismo no começo do século XX (TARDE, 2005), até as atuais polarizações público-privado com as redes sociais como *Facebook*, podemos verificar o problema em circulação. Os fenômenos de midiatização (HEPP, 2013) ao longo da história tendem a reconfigurar o que se entende por privacidade. Na atual sociedade da informação, acredita-se que o conceito está ligado à habilidade de uma pessoa em controlar a exposição e a disponibilidade de dados acerca de si. Como diz Tulio Viana (2006, p. 116):

> O direito à privacidade, concebido como uma tríade de direitos–de não ser monitorado, de não ser registrado e de não ser reconhecido (direito de não ter registros pessoais publicados)–transcende, pois, nas sociedades informacionais, os limites de mero direito de interesse privado para se tornar um dos fundamentos do Estado Democrático de Direito.

A ITU (2005, p. 7, tradução nossa) destaca cinco dimensões da privacidade:

> A privacidade permite que as pessoas controlem informações sobre si mesmas; A privacidade protege as pessoas contra perturbações indesejadas; Privacidade é o direito de ser deixado em paz; Privacidade é obrigação recíproca de divulgação entre as partes; A privacidade é um agente regulador que pode ser usado para balancear e verificar o poder de quem é capaz de coletar dados.[8]

Podemos entender a privacidade enquanto uma dimensão maleável, ganhando maior ou menor importância em diversas práticas

8 Privacy empowers people to control information about themselves; Privacy protects people against unwanted nuisances; Privacy is the right to be left alone; Privacy is reciprocal obligations of disclosure between parties; Privacy is a regulating agent that can be used to balance and check the power of those capable of collecting data.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

sociais, desde conversar com um ente querido presencialmente, falar ao telefone, enviar um e-mail, uma mensagem via *WhatsApp*, ou com a IoT, a partir da popularização de dispositivos domésticos inteligentes (como lâmpadas conectadas e *smart speakers*, no espaço da casa, ou o uso de *wearables*, traduzindo, analisando e compartilhando dados pessoais corporais), por exemplo. Ela se apresenta como uma dimensão mais ou menos relevante a depender de contextos específicos[9]. Essa maleabilidade situa a questão da privacidade desde sempre. Ela vai adquirindo, ao longo da história do desenvolvimento dos humores sociais, das mídias e tecnologias de comunicação e informação, contornos particulares. Portanto, entendimentos sobre o que é e quais os limites da privacidade são contextuais e contingenciados por diversos campos da vida social (DECEW, 1997; PARKER, 1973; SOLOVE, 2002; WESTIN, 1984) e os sujeitos têm preocupações e entendimentos diferenciados em relação à questão (PONCIANO et al., 2017). Poderíamos acrescentar, também, que a privacidade sempre é produzida a partir de múltiplas mediações, de forma sempre relacional através de agenciamentos materiais (FOX; ALLDRED, 2016). A maleabilidade e transitoriedade do conceito de privacidade, portanto, reforça a necessidade de observar como o mesmo é produzido, percebido e circulado, para além de enquadrá-la em perspectivas essencialistas.

A diferença entre a percepção da gravidade do problema e a forma como se comportam os indivíduos caracterizam o "paradoxo da privacidade". Como dito anteriormente, os agenciamentos e as relações materiais produzirão diferentes paradoxos da privacidade ao longo do tempo e das redes às quais a questão aparece. No caso dos sistemas computacionais, por exemplo, é comum que usuários se posicionem como preocupados em relação à circulação de suas informações pessoais e, ao mesmo tempo, sujeitem-se à utilidade dos sistemas, compartilhando dados para ter serviços em redes sociais digitais (KEHR et al., 2015; KOKOLAKIS, 2017; OETZEL; GONJA, 2011; WAKEFIELD, 2013).

Uma análise a partir da SP pode nos ajudar a verificar quais condições materiais específicas agenciam os usuários a permitir

9 Solove (2002) ilustra essa maleabilidade com o caso da percepção e prática de proteção à privacidade no sistema de correio americano. Graças à falta de segurança dos selos de cera das cartas, criou-se um clima de suspeita sobre os funcionários das empresas postais que, potencialmente, estariam lendo o conteúdo, particularmente de cartas de figuras públicas. Isso levou à produção de códigos para a escrita das cartas, alterando de forma significativa a sua forma de comunicação. O fenômeno fomentou o desenvolvimento de aprovação de diversas leis que proibiam a abertura imprópria de cartas, dentre outras questões.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

a coleta e processamento de seus dados pessoais, mesmo com ressalvas e preocupações – o paradoxo. Os dispositivos de modulação de comportamento (SILVEIRA, 2017), orientados a uma ideia de capitalismo de dados (SRNICEK, 2017), ou de vigilância (ZUBOFF, 2015), buscam estratégias de invisibilidade e/ou de naturalização desses procedimentos, produzindo um encaixapretamento dos aparatos de violação da privacidade. Em outras palavras, a assimetria de conhecimento entre usuário e plataforma não está dada *a priori*, mas é produzida materialmente em rede. A presença de padrões interfaciais maliciosos (BÖSCH et al., 2016; DIETER, 2015; GRAY et al., 2018) em aplicativos de uso diverso, e mesmo produtos da IoT, ajudam a revelar as condições de instauração do paradoxo da privacidade.

Ao longo da última década, com a proliferação de bens de consumo conectados à internet, os problemas de privacidade ganharam expressividade mercadológica, política, legal e social, amplificando o número de estudos que se debruçam sobre o fenômeno (BUNZ, 2016; CHRIST; WINTERTHUR, 2015; KARIMOVA; SHIRKHANBEIK, 2015; NANSEN et al., 2014). Há um interesse majoritário em avaliar duas grandes questões: a) Quais são os potenciais riscos e ameaças para a manutenção da vida privada?; b) Quais alterações a crescente presença dessas tecnologias produz no entendimento dos limites entre público e privado? Aleisa e Renaud (2017) reforçam a expectativa do usuário em relação à proteção dos dados pessoais. Segundo sua pesquisa, o rastreamento dos dados por terceiros aparece como uma das principais preocupações apontadas pela literatura (31.5%), principalmente no que diz respeito à localização do usuário. Destacam-se ainda o compartilhamento de dados identificáveis com terceiros (26%) e perfilização (21%) como ameaças significativas. Observaremos a seguir como algumas dessas questões se manifestam numa das marcas mais bem-sucedidas da IoT global – a Nest.

Sobre os fluxos de dados na rede Nest

Os objetos da empresa Nest correspondem a alguns dos mais bem-sucedidos bens de consumo da IoT[10]. Trata-se de um amplo ecossistema de aparelhos: termostatos e sensores de temperatura, câmeras de vigilância, campainhas com câmeras embarcadas, sistemas de alarme, fechaduras e detectores de fumaça. Ao total, o portfólio da empresa

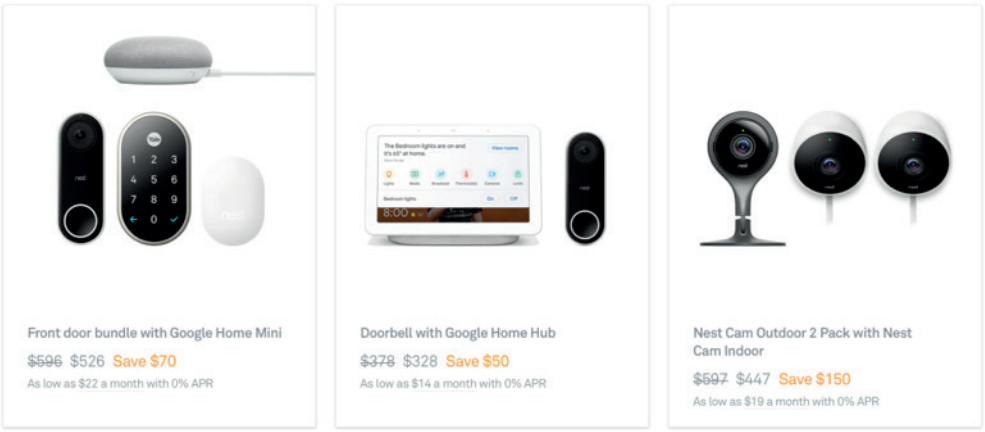
10 O Nest é um pioneiro na área e um dos melhores atualmente no mercado da IoT, tendo obtido reconhecimento internacional a partir da comercialização de termostatos inteligentes, um dos primeiros bens de consumo a ganhar expressividade mercadológica (cnet.com/topics/smart-home/best-smart-home-devices/best-smart-thermostats). Entretanto, especula-se que a marca, recentemente adquirida pelo conglomerado Alphabet, esteja dando prejuízo: cnbc.com/2017/06/28/alphabet-tried-selling-nest-in-2016-after-paying-3-point-2-billion-in-2014.html

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

é composto por 14 produtos diferentes, todos estes, enquanto objetos da IoT, possuindo capacidades infocomunicacionais e algorítmicas que os diferenciam das versões analógicas da mesma categoria. Além dos produtos físicos, a Nest também oferece Aplicativos Móveis (APPS) para o gerenciamento e a configuração desses objetos, além de serviços de hospedagem e de monitoramento 24/7 em nuvem (Nest Aware). Há um esforço comercial por parte da empresa em convencer o consumidor a adquirir múltiplos e diferentes produtos, tendo em vista sua interoperabilidade. Esse esforço é verificável na seção "*Offers*"[11], em destaque na página oficial da marca, na qual pacotes de produtos são anunciados – *bundles* – (Fig. 1) e destinados a otimizar o uso em conjunto. Alguns desses pacotes incluem, inclusive, produtos de marcas parceiras, como o Google Home Mini e o Google Home Hub. É importante ressaltar que a Nest compõe formalmente o conglomerado Alphabet desde 2014, quando foi adquirida por 3.2 bilhões de dólares. Em 2018, a empresa deixa de operar de forma independente e passa a integrar o conglomerado de hardware da Google[12].

Figura 1: Pacotes de produtos Nest.



Fonte: Disponível em: <https://nest.com/offers/>. Acesso em: 03 jul. 2018.

11 Ver mais em: <https://nest.com/offers>.

12 Ver mais em: <https://www.reuters.com/article/us-alphabet-nest/alphabet-shifts-thermostat-maker-nest-into-google-idUSKBN1FR343>.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

Na pesquisa empírica desenvolvida por Dirkzwager et al. (2017),[13] é possível verificar quais dados pessoais são retirados de dispositivos que integram a família Nest e como eles potencialmente circulam entre parceiros. Os autores partem de uma análise de documentos oficiais da Nest (políticas de privacidade, termos de uso e informações do site) para identificar uma média de 24 tipos de dados coletados pelos diferentes dispositivos. Além disso, o estudo aponta para a existência de 116 parceiros da marca que podem se conectar e receber dados coletados pelos dispositivos, desde aspectos técnicos da rede (IP, endereço de e-mail, dados de *bluetooth* etc.), dimensões físicas do espaço (temperatura, umidade etc.) e padrões comportamentais dos usuários (horários, movimento no espaço doméstico, temperatura favorita etc.)[14]. Dentre os 116 parceiros mapeados, é possível encontrar uma variedade de produtos e serviços tais como: *smart speakers*, *wearables*, lâmpadas inteligentes, eletrodomésticos etc. A preocupação dos autores está na invisibilidade dos processos de circulação e de gerenciamento de dados pessoais, bem como à pouca atenção dada às questões de segurança.

O trabalho de Dirkzwager et al. (2017) nos ajuda a materializar os problemas de privacidade no âmbito da IoT e mostrar a agência da SP nesse sistema. A rede do termostato Nest (Fig. 2) descreve o que acontece com a circulação dos dados pessoais, passando pela ação direta do usuário, da sensibilidade do objeto em captar dados do ambiente e de outros objetos – seus sensores e materialidades –, e das agências futuras em outros bancos de dados (performatividade) e influência nas narrativas publicitárias, coleta de dados de empresas parceiras, inteligência de negócios proveniente da análise dos dados (*big data*) etc.

Podemos identificar no diagrama acima os sete problemas de privacidade de acordo com a proposição de Ziegeldorf et al. (2014) e como eles se posicionam nessa rede – marcados em amarelo na Figura 2. Esses sete problemas nos permitem mapear os quatro pontos centrais da privacidade (coleta de dados, inferências, compartilhamento

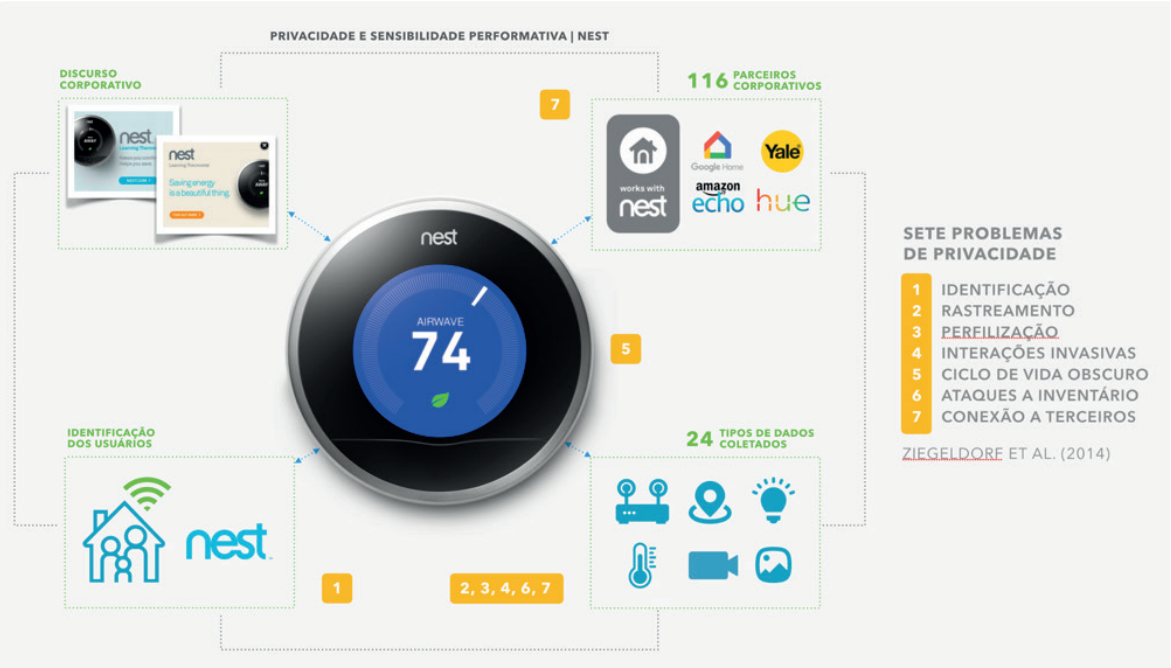
13 A pesquisa realizada é especulativa e visa ilustrar o potencial de violação da privacidade. Os autores não afirmam categoricamente que existe uma circulação intensa, ou coleta de dados pessoais.

14 O usuário fornece dados de referência pessoal e o objeto estuda seu comportamento, aprendendo, por exemplo, a temperatura preferida para a casa. Usando sensores integrados e geotracking, o termostato 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.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

Figura 2: Rede da SP do termostato Nest, dados coletados e compartilhamento de informações pessoais.



Fonte: Dos autores (2019)

e paradoxo da privacidade[15]) identificados por Ponciano et al. (2017), que serão discutidos mais adiante.

O primeiro dos problemas é a identificação (1), ou seja, a capacidade de relacionar dados a indivíduos específicos. Ela surge na rede a partir do espaço doméstico e dos usuários envolvidos com o dispositivo, mas espalha-se através da coleta de dados que geram a identificação e compartilhamento de informações com os parceiros comerciais. A capacidade de rastreamento, entendida como a habilidade da rede de determinar e memorizar a localização dos indivíduos ao longo do espaço-tempo se apresenta como o segundo problema (2), a medida em que os dados coletados produzem padrões e memorizam o histórico de uma interação senciente. O sistema também perfiliza (problema 3) os usuários, produzindo entendimentos contextualizados e ações futuras sobre seu comportamento, revelando padrões de deslocamento e comportamento no ambiente doméstico. Isso se agrava ao

15 No caso do "paradoxo da privacidade", estudos mais concretos com usuários devem ser feitos para indicar como exatamente esse problema ocorre.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

pensarmos na realização de interações invasivas (problema 4) que possam violar a privacidade ao publicizar informações íntimas, tanto para parceiros comerciais, quanto para outros usuários presentes na mesma rede.

Destacam-se também problemas relacionados ao ciclo de vida do produto (problema 5), tendo em vista que os dados coletados e padrões inferidos pelo dispositivo circulam sem muito controle em diferentes momentos da vida do objeto (desde a sua produção até o descarte)[16]. Essa questão aponta tanto para o gerenciamento material dos dados (sua manipulação direta pelos actantes envolvidos), bem como para a (in)visibilidade nas políticas de privacidade da empresa, um perigoso binômio apontado por Pasquale (2015): as empresas produzem sofisticados dispositivos de coleta e vigilância que, paradoxalmente, não são passíveis de acesso e/ou escrutínio pela sociedade civil.

A ampla conectividade da rede Nest também aponta para problemas de ataques de inventário (problema 6) e de combinação de dados com outros sistemas (problema 7). O primeiro se refere a capacidade de obter dados e informações pessoais através da interconectividade de múltiplos dispositivos. Através de uma lâmpada conectada a rede Nest, seria possível obter dados sobre o último, por exemplo. O segundo aponta para a combinação de bases de dados de diferentes dispositivos, amplificando o risco de identificação do usuário a partir de informações isoladas.

Casos como o retratado acima reforçam a necessidade de reflexão e aferição sobre como a IoT tensiona as esferas de controle pública e privada dos indivíduos. Essa demanda se torna ainda mais urgente ao compreendermos que o compartilhamento não autorizado de informações com terceiros (PONCIANO et al., 2017) se configura enquanto principal ameaça percebida por usuários de produtos inteligentes. A invisibilidade dos algoritmos e dos dispositivos IoT produzem, nesse sentido, uma falsa percepção de que o sujeito mantém controle sobre sua privacidade. Uma ampla rede de agências entra em ação, precisando ser estudada para entendermos os desafios da privacidade na IoT.

É sabido que, mesmo através de dados aparentemente pouco sensíveis – como

16 Descobriu-se recentemente que carros autônomos da marca Tesla servem como repositórios de dados após seu descarte. Pesquisadores foram capazes de minerar informações pessoais sensíveis a partir de modelos abandonados em um ferro-velho nos Estados Unidos. Ver <https://www.cnbc.com/2019/03/29/tesla-model-3-keeps-data-like-crash-videos-location-phone-contacts.html>.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

metadados de navegação –, é possível identificar os usuários, tornando-os alvo de práticas econômicas pós-industriais – capitalismo de dados –, pautadas na coleta, processamento e análise de dados pessoais com a finalidade de modular comportamentos. Embora a preservação da privacidade possa existir como paradigma em diferentes produtos IoT (*privacyby design*), entendemos que a lógica de mercado está permanentemente em tensão com esse aspecto. As empresas devem levar em consideração as consequências legais/financeiras de não olhar para a privacidade, já que há um nítido contraste entre o nível de privacidade que o mercado prioriza (que busca de alguma forma economia e remontar do "dividual" ao individual) e a ideia de privacidade que os contratos sociais exigem em sociedade democráticas.

A privacidade no contexto da Internet das Coisas: apontamentos a partir do caso Nest

A partir do exposto, vamos mostrar como a rede de SP na IoT nos ajuda a identificar controvérsias acerca da privacidade. Para tanto, tomaremos como ponto de partida quatro pontos centrais destacados por Ponciano et al. (2017) como as maiores ameaças à privacidade com o desenvolvimento da IoT. São eles: A coleta indiscriminada de dados pessoais; a inferência de novas informações através do cruzamento de dados e *machine learning*; a troca e compartilhamento de informações com terceiros e; a percepção de utilidade do produto em detrimento do risco de sua utilização – paradoxo da privacidade.

Coleta de dados pessoais

Essa é a porta de entrada para a IoT e para a rede a partir da SP. O sensor, que está na base do objeto "inteligente", começa sua ação ao sentir uma grandeza física e transformá-la em dados que serão compartilhados com outros objetos em rede. A escolha de qual grandeza física será transformada em dados, e como esses dados serão processados, já coloca a SP no cerne do problema da privacidade. Essa escolha nunca é neutra e, como revela a rede apontada no exemplo da Nest, a invisibilidade dos sistemas computacionais esconde uma coleta de dados muito maior. Um usuário comum não consegue nomear os 24 tipos de dados coletados pelo termostato[17], ou mesmo justificar a necessidade dessa coleta. Nesse caso e em muitos outros ligados a objetos

17 A dimensão de coleta de dados não é particularidade da IoT, já que a emergência de tecnologias de informação e comunicação produz formas inéditas, e cada vez menos transparentes, de coleta e processamento de informações.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

de uso massivo[18] da IoT, a ação se dá em um contexto muito particular, pessoal e muitas vezes no espaço privado e em um regime ininterrupto.

Com a IoT, há um aumento quantitativo e qualitativo no que tange a coleta de dados pessoais (ZIEGELDORF, 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. É o que Jones (2015) chama de "Internet das Coisas dos Outros". A grande quantidade de parceiros presentes na rede Nest reafirma essa questão. A mudança qualitativa, por sua vez, diz respeito à crescente variedade de dados e informações pessoais que passam a ser passíveis de coleta – novos *data sets* – fazendo com que a SP funcione de forma mais espraiada e cada vez menos transparente. Entra em questão aqui a materialidade do dispositivo, a transparência das suas interfaces e a política industrial das empresas desenvolvedoras.

Objetos inteligentes no espaço urbano (*smart city*), no espaço privado (*smart homes*) ou colados ao corpo (*wearables*) têm formas ampliadas de coleta, quantificação e processamento de informações pessoais, publicizando dados que, outrora, seriam considerados íntimos. Mesmo que o uso não seja personalizado, os dados captados entram em regime de circulação, pois são compartilhados em *data centers*, servem para gerar prognósticos (*big data*) e fazem outros objetos agirem de acordo (parceiros comerciais), ou vão criar narrativas institucionais como "o espaço urbano ficará mais eficiente", "a casa será mais segura", ou o "usuário terá mais saúde". No caso do Nest, o bordão publicitário é: "*Saving energy is a beautiful thing*". Esses discursos, por sua vez, modulam comportamentos orientados à produção de dados e ao questionamento da privacidade. Portanto, é possível ver como a SP, a partir do problema da coleta de dados, afeta questões de privacidade. A heterogeneidade de dispositivos, dados e estratégias de coleta e processamento, portanto, produzem não só novas concepções sobre o público e o privado, mas engajam os sujeitos na construção de diferentes práticas de privacidade (SOLOVE, 2002).

18 Por uso massivo da IoT entendemos os objetos de consumo em venda no mercado, tais como lâmpadas inteligentes, sensores, termostatos, fechaduras, caixas de som, *wearables*, dentre outros. Nosso interesse é discutir a privacidade no contexto desses objetos e não naqueles que envolvem M2M industrial ou equipamentos urbanos nas "cidades inteligentes". Para esse último aspecto, ver Lemos e Jesus (2017).

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

Inferência de novas informações

Como vimos, a SP não se limita ao sensor, ou ao atuador no objeto. Ela constitui a IoT como um ator-rede desenvolvendo uma agência de amplo alcance. A informação captada pode ser utilizada em recombinações futuras. Como aponta Kitchin (2014), dados não indexais em grandes quantidades podem ser unidos e rastreados através de identificadores compartilhados. Isso permite discriminação, combinação, desagregação e reagregação, busca e outras formas de processamento e análise. Ponciano et al. (2017) colocam essa preocupação como a inferência de novas informações a partir do processamento algorítmico (FINN, 2017) e *machine learning*. Assim, objetos da IoT poderiam, até determinado ponto, produzir conclusões e inferências sobre o sujeito a partir das informações performadas pela SP. Sua ação amplia a performatividade do objeto com a afetação de informações de outros objetos (parceiros conectados ao Nest) que gerarão informações e ações sobre esse indivíduo. E tudo isso sem que ele tenha conhecimento, ou mesmo tenha autorizado conscientemente o procedimento.

Por exemplo, um dado sobre batimento cardíaco captado por 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 de relaxamento em que se encontra o usuário[19]. Ao utilizar um objeto que mede os batimentos cardíacos, a primeira intenção do usuário é monitorar seu coração. No entanto, a SP produz agências amplas sem que o usuário se dê conta. O mesmo pode ser dito em relação ao Nest. A variedade – e qualidade – de dados coletados em conjunto, a ampla capacidade de conectividade do produto com outros aparelhos amplia a capacidade da SP de ameaçar a privacidade. O discurso mercadológico da "família" de produtos aponta para essa prática: a convergência do termostato, câmera de vigilância e detector de fumaça (todos da marca Nest) no mesmo ambiente amplia a coleta de dados e seu potencial de cruzamento. Portanto, à medida que o espalhamento de objetos IoT se estende para o corpo, para o lar, ou para as práticas de consumo, a rotina dos sujeitos e os padrões tornam-se mais visíveis aos algoritmos do que para o próprio usuário.

19 Recentemente pesquisas em psicologia afirmam que seria possível, com base em alguns posts no *Facebook*, identificar o estado psicológico de uma pessoa. Isso pode ser utilizado por empresas para sugerir compras impulsivas dado o estado atual de um indivíduo. Ver matéria do *Telegraph*: This online tool reveals your personality based on Facebook 'likes'. 2015. Disponível em: < https://www.telegraph.co.uk/technology/facebook/11838515/This-online-tool-reveals-your-personality-based-on-Facebook-likes.html>. Acesso em: 28 maio 2018.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

Compartilhamento de informações com terceiros

Outra grande fonte de preocupação acerca da privacidade na IoT diz respeito ao compartilhamento indiscriminado de informações pessoais com terceiros. Uma das facetas da SP é agir também nesse nível, tendo em vista que sua ação começa no sensor e vai se alargando para objetos e sistemas muito mais amplos. Assim, preocupações sobre a privacidade emergem não só quando do acesso de dados pessoais por parte das empresas diretamente envolvidas, mas principalmente pelas empresas parceiras destas (BUCHENSCHEIT et al., 2014; KNIJNENBURG; KOBSA, 2014) e pelos governos (PONCIANO et al., 2017). O compartilhamento de dados servirá para fazer com que o usuário não seja o único receptor do dado coletado e processado (*data recipient*), e que as informações sirvam para práticas diversas de perfilização (*profiling*) e identificação pessoal.

O que está em jogo é a constituição de uma rede de processos opacos e pouco compreensíveis para o usuário comum. Há, assim, a ausência do que Ziegeldorf et al. (2014) chamam de "autodeterminação informacional" (*informational self-determination*), ou seja, a capacidade do sujeito em avaliar os riscos para a garantia da sua 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. Se a SP da IoT age em um fundo pouco visível, como essa autodeterminação informacional pode ocorrer? É necessário, portanto, pensar nas dimensões ético-moral, jurídica e educativa da SP, já que não há clareza sobre a captura (I), a inferência de novos dados (II), nem sobre quais e como as informações são compartilhadas com terceiros (III).

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. No entanto, como sustentamos, a SP como um princípio dos objetos da IoT deve ser entendida não propriamente como uma fronteira, mas como um conjunto de performatividades específicas entre bordas, envolvendo diversos objetos, sistemas e pessoas. Quando um sistema coleta dados, cruza com outros e gera compartilhamento, não se trata tanto de bloquear ou criar fronteiras, mas de estipular as formas de agência e os tipos de performatividade algorítimica que estarão em jogo. Assim, politizar as fronteiras informacionais requer observar como as performatividades algorítmicas e outras instâncias materiais produzem agenciamentos (relacionais) e, nessas afetações, produzem instâncias públicas e/ou privadas (FOX; ALLDRED, 2016). Interessa entender como as múltiplas agências rastreadas pela SP torcem, borram e produzem fronteiras informacionais.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

A indicação que a cada indivíduo é dada a possibilidade de se engajar em um processo dinâmico de "abertura" e "fechamento" do acesso às suas informações pessoais é interessante, mas difícil de ser concretizada, dada a indeterminação do fluxo da informação em sistemas de IoT. Em tese parece ser possível, como sustentam Ponciano et al. (2017), a produção de fronteiras fluidas que delimitarão o acesso aos dados e que cada sujeito possa trabalhar em prol da definição de regras específicas que definirão o movimento dessas fronteiras. A delimitação das fronteiras de acesso – ou das esferas de controle – no cenário da IoT é muito mais complexa. É muito difícil ter clareza sobre os riscos e benefícios (paradoxo da privacidade). Como já dito, essa dificuldade é projetada (*by design*), tendo em vista o grande potencial do mercado de dados pessoais e capitalismo de plataforma (SRNICEK, 2017).

Em grande medida, graças ao regime de invisibilidade dos dispositivos e algoritmos coletores de dados, não há transparência sobre o que pode estar sendo coletado e quando a coleta acontece. Seria mais interessante politizar as performatividades das bordas entre objetos e sistemas. Por politizar entendemos a necessidade de trazer à luz os procedimentos algorítmicos, a agência dos dados desempenhada pela SP na IoT, sem perder de vista a discrepância de conhecimento entre agentes humanos e não humanos no sistema (PASQUALE, 2015). Essa questão remonta tanto para a dimensão interfacial dos produtos, quanto para as políticas comerciais das empresas. Dispositivos como o Nest escapam ao repertório de interação da maioria de usuários – habituados com o paradigma computacional da interface gráfica de usuário –, dificultando o entendimento sobre as práticas de dado. Multiplica-se a capacidade de interconexão dos produtos, enriquecendo o processo de coleta de dados.

Dado o caráter opaco e pouco transparente dos sistemas de IoT, os objetos conectados e atuantes a partir da SP terão mais informações sobre as pessoas do que as pessoas sobre os sistemas, o que torna a questão da privacidade crucial. Iluminar os procedimentos algorítmicos, nesse sentido, pressupõe observar sua agência e causalidade em sistemas IoT, mais precisamente a afetação nas práticas cotidianas de privacidade. A porosidade de borda está além da possibilidade de decisão e de controle por parte do sujeito.

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, menor serão

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

as preocupações do usuário com problemas de privacidade (PONCIANO et al., 2017), reforçando o paradoxo da privacidade. As pessoas se preocupam com a privacidade, mas, mesmo assim, oferecem informações pessoais, correndo riscos. Certamente, esse paradoxo varia de acordo com a experiência dos usuários, a usabilidade e o design dos dispositivos, a percepção dos riscos, as normas sociais e o discurso produzido pelas empresas. Embora esse fenômeno exista em outras dimensões da Internet (BARTH; DE JONG, 2017; KOKOLAKIS, 2017; LI et al., 2016; LUTZ; STRATHOFF, 2014; OETZEL; GONJA, 2011), cabe observar suas particularidades no contexto específico da IoT.

Williams et al. (2016), por exemplo, acreditam que o desenvolvimento da IoT amplificará esse paradoxo. O argumento dos autores toma como base os aspectos específicos da SP, particularmente aqueles que se relacionam às interfaces dos produtos – como apontado acima no caso do Nest –, a ubiquidade da coleta de dados e a ação do mercado. Entende-se que a heterogeneidade de produtos inteligentes, e suas múltiplas interfaces, dificultam a usabilidade. Como consequência, parcelas significativas de usuários IoT não realizam ações simples de proteção dos seus dados, como alterar a senha padrão dos aparelhos por dificuldade de acesso. A invisibilidade das trocas informacionais posta em marcha pela SP – aliada à ausência de compreensão sobre as interfaces – contribuirá para um baixo entendimento sobre como, quando e de que forma os dispositivos coletam e processam dados pessoais. Por um lado, não se sabe, logo o problema não aparece. Por outro, pode-se saber, mas esse conhecimento é negligenciado em nome da usabilidade do objeto (o paradoxo, portanto).

A dimensão mercadológica contribui para o aprofundamento do paradoxo. O contínuo lançamento de produtos não privilegia investimentos em segurança, ou opções de configuração de privacidade, dada a necessidade de baratear custos. 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 et al., 2017), Williams et al. (2016) destacam que a necessidade de lançar produtos novos e mais baratos interfere na lógica da qualidade.

No nosso exemplo, vemos que a Nest inicia as atividades como um termostato e hoje comercializa câmeras de vigilância, campainhas, alarmes, fechaduras e detectores de fumaça. O grande número de parceiros comerciais (116) aponta para a proliferação de novos produtos no mercado, produzindo um ambiente de alta

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

competitividade. Para o usuário, se tudo se integra bem, melhor, negligenciando a proteção de dados pessoais, seja pelo desconhecimento, seja pela ação do paradoxo da privacidade. Para o mercado, o que mais tem valor é o dado do usuário, sendo esse o modelo de negócio que pauta a comercialização: troca e análise de dados pessoais, principalmente para a indústria da publicidade e e-commerce (SILVEIRA, 2017b). Os atuais fenômenos como a perfilização só são possíveis graças a essa lógica.

Considerações finais

A questão da privacidade na IoT deve ser entendida de forma ampla, partindo do reconhecimento da SP como um princípio desses objetos. A SP produz um conjunto de ações, uma "comunicação das coisas" (LEMOS, 2013) que afeta o objeto em suas mais diversas dimensões: uso, interface, troca de dados, mercado, publicidade etc. A privacidade é uma das questões que emergem a partir do agenciamento da SP. 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, são questões interligadas à performance algorítmica da sensibilidade infocomunicacional desses objetos.

Cabe apontar que a discussão acerca da privacidade no que tange a SP vai além da questão da vigilância (BEZERRA, 2017; RADFAHRER, 2018), bem como das situações de interação e exposição de si (AYRES; RIBEIRO, 2018). Dessa forma, mapear e problematizar a privacidade no contexto da mediação algorítmica requer o rastreamento de ação da SP, bem como o escrutínio das condições materiais sua de produção (DOURISH, 2017; FOX; ALLDRED, 2016). Reforçando o entendimento de Solove (2002), a SP demonstra como as práticas de privacidade são efetivamente construídas por diferentes instâncias, partindo da engenharia do sensor embarcado até a narrativa publicitária, veiculada em meios de comunicação de massa. Cada uma dessas instâncias provoca, consequentemente, novas questões e tensões que vão aos poucos moldando o entendimento sobre dados pessoais e como as ações são engendradas para cedê-los ou protegê-los. Compreender os dilemas da privacidade é ressaltar essa rede de agências da SP dos objetos da IoT, sendo uma das questões prioritárias da atual cultura digital.

Vimos isso na rede Nest. O produto é colocado em um ambiente para controlar automaticamente e inteligentemente a temperatura do espaço privado interno. A SP vai se espraiar como uma rede que pode ser compreendida em suas mais diversas partes: a funcionalidade do objeto, a interface

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

gráfica de comando, os dados que ele retira do ambiente e como o modelo de negócio e o discurso publicitário para sua venda destacam a eficiência energética e a segurança da casa. O dispositivo coleta dados do espaço, indicando como as pessoas se comportam ao longo do tempo, as preferências de turnos e estações, quando é ligado ou desligado, apontando presença ou ausência em lugares específicos do recinto. Mais ainda, as informações estão sujeitas a cruzamentos e inferências quando compartilhadas com empresas e bancos de dados, podendo projetar perfis futuros, ou em tempo real.

Entendendo a privacidade como um direito inalienável de proteção de dados pessoais[20], algumas questões devem ser postas: Quais e como os dados são coletados? Com que finalidade? O usuário tem informação sobre essas ações? Para quais empresas ou instituições governamentais eles são enviados? Como e por quanto tempo eles são armazenados? Quais as formas de ação posterior sobre o sujeito ou outros objetos pessoais? A resposta a essas perguntas pode, pela ação da SP na IoT começar por qualquer ponto da rede: analisando o discurso publicitários chegamos ao sensor, e a partir dos dados coletados é possível problematizar interface e compartilhamento, e assim sucessivamente. Compreender a questão da privacidade é destacar um olhar sobre essa rede em deslocamento.

Não é nossa intenção, neste trabalho, o aprofundamento das soluções, mas podemos apontar que certamente elas se darão nos aspectos jurídicos, em alternativas de privacidade pelo design e em uma politização (educação) tornando visíveis as ameaças envolvidas e forçando os padrões de segurança a serem adotados pelas indústrias. De acordo com Hoepman (2012), tratam-se de estratégias que, por um lado, lidam com 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* – precisa abarcar esses dois polos. Algumas soluções devem ser enquadradas em um sistema legal, ou práticas de privacidade embarcadas no projeto dos produtos. Deve-se tornar confiável a circulação dos dados e a origem dos objetos. Soluções

20 Essa questão se torna ainda mais relevante frente à implementação do Regulamento Geral de Proteção de Dados na União Europeia (o GDPR, acrônimo em inglês). Como os analistas apontam, o escrutínio acerca das políticas de coleta e uso de dados pessoais impõe múltiplas controvérsias ao modelo de operação das instituições na internet. Para mais detalhes, acesse: <https://www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe>.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

de redes federadas e/ou *blockchains*[21] podem ser modelos interessantes a serem desenvolvidos. São fundamentais o desenvolvimento e a melhoria dos padrões de segurança a serem adotados pelas indústrias e a implantação de interfaces de configuração amigáveis nas quais os ajustes de privacidade sejam claros e transparentes.

Por fim, é fundamental politizar o debate, entendendo o papel dos objetos e da nova performatividade algorítmica. Alguns autores apostam que os objetos poderão, de forma autônoma, encontrar parceiros em uma espécie de rede social de objetos, ampliando as ameaças à privacidade (KARIMOVA; SHIRKHANBEIK, 2015). É importante compreender que há uma crescente fetichização dos algoritmos e dos sistemas computacionais para produzir uma aura de confiabilidade (FINN, 2017; SILVEIRA, 2017a). Um dos efeitos colaterais é o que Danaher (2016) chama de "algocracia", ou seja, a organização de tomada de decisões a partir de ações tecnocráticas e burocráticas baseadas na "neutralidade" dos algoritmos. Nesse sentido, à medida que a visão idealizada da IoT – um mundo totalmente interconectado e regido pela inteligência algorítmica – caminha em direção à realidade, diferentes problemas de ataque à privacidade aparecem e convergem, ameaçando a manutenção do contrato social (OWEN, 2015).

Referências

ALEISA, Noura; RENAUD, Karen. Privacy of the Internet of Things: A Systematic Literature Review. **Proceedings of the 50th Hawaii International Conference on System Sciences**, p. 5947-5956, 2017.

AUSTIN, John Langshaw. **How to Do Things with Words.** Clarendon Press, Oxford, 1962.

AYRES, Marcel; RIBEIRO, José Carlos. A dimensão informacional na regulação do contexto de privacidade em interações sociais mediadas por dispositivos móveis celulares. **Intercom: Revista Brasileira de Ciências da Comunicação**, v. 41, n. 1, p. 81-97, 2018.

BARAD, Karen. **Meeting the Universe Halfway:** Quantum Physics and the Entanglement of Matter and Meaning. Durham e London: Duke University Press, 2007.

BARTH, Susanne; DE JONG, Menno D. T. The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior; A systematic literature review. **Telematics and Informatics**, v. 34, n. 07, p. 1038-1058, 2017.

BEZERRA, Arthur Coelho. Vigilância e cultura algorítmica no novo regime global de mediação da informação. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 22, n. 4, p. 68-81, 2017.

21 Ver *IoT and Blockchain: Challenges and Risks*. Disponível em <https://www.bbvaopenmind.com/en/iot-and-blockchain-challenges-and-risks>. Acesso em: 30 jan. 2018.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

BÖSCH, Christoph. et al. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. **Proceedings on Privacy Enhancing Technologies**, v. 2016, n. 4, jan. 2016. Disponível em: <http://content.sciendo.com/view/journals/popets/2016/4/article-p237.xml>. Acesso em: 12 jul. 2018.

BRANDEIS, Louis; WARREN, Samuel. The Right to Privacy. **Harvard Law Review 4**, v. IV, n. 5, p. 193-220, 1890.

BUCHENSCHEIT, Andreas. et al. Privacy implications of presence sharing in mobile messaging applications. **Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia–MUM '14**, v. 1, n. 1, p. 20-29, Dec. 2014.

BUNZ, Mercedes. The Internet of Things: tracing a new field of enquiry. **Media, Culture & Society**, v. 38, n. 8, p. 1278-1282, 2016.

CAVOUKIAN, Ann; JONAS, Jeff. **Privacy by Design in the Age of Big Data**. Information and Privacy Commissioner of Ontario, 2012. Disponível em: < https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf >. Acesso em: 03 jul 2018.

CHENEY-LIPPOLD, John. **We Are Data**. New York: NYU Press, 2017.

CHRIST, Oliver. Martin Heidegger's Notions of World and Technology in the Internet of Things age. **Asian Journal of Computer and Information Systems**, v. 3, n. 2, p. 58-64, 2015.

DANAHER, John. The Threat of Algocracy: Reality, Resistance and Accommodation. **Philosophy and Technology**, v. 29, n. 3, p. 245-268, 2016.

DECEW, Judith Wagner. **In pursuit of privacy: law, ethics, and the rise of technology**. Ithaca: Cornell University Press, 1997.

DELEUZE, Gilles. Posdata sobre las sociedades de control. In: FERRER, Christian (Comp.). **El linguaje libertario:** Antología del pensamiento anarquista contemporáneo. Buenos Aires: Altamira, 1999.

DIETER, Michael. Dark Patterns: Interface Design, Augmentation and Crisis. In: BERRY, David M.; DIETER, Michael. (Org.). **Postdigital Aesthetics**. London: Palgrave Macmillan UK, 2015. p. 163-178. Disponível em: <http://link.springer.com/10.1057/9781137437204_13>. Acesso em: 30 abr. 2019.

DIJCK, Jose van; POELL, Thomas; WAAL, Martijn de. **The Platform Society**. New York: Oxford University Press, 2018.

DIRKZWAGER, Aimee; CORNELISSE, Jimi; BROK, Tom; CORCORAN, Liam. **Where does your data go?** Mapping the data flow of Nest. Masters of Media, 2017.

DOTY, Nick; GUPTA, Mohit. Privacy Design Patterns and Anti-Patterns Patterns Misapplied and Unintended Consequences. Proceedings of the Ninth Symposium on Usable Privacy and Security, v.1, n.1, p. 1-5, 2013.

DOURISH, Paul. **The Stuff of Bits**. Cambridge: MIT Press, 2017.

DOURISH, Paul; GÓMEZ CRUZ, Edgar. Datafication and Data Fiction: Narrating Data and Narrating with Data. **Big Data & Society**, v. 5, n. 2, p. 1-10, jul. 2018.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

FINN, Ed. **What Algorithms Want:** Imagination in the Age of Computing. Cambridge: MIT Press, 2017.

FOUCAULT, Michel. **Microfísica do poder**. 2. ed. Rio de Janeiro: Paz e Terra, 2015.

FOX, Nick J.; ALLDRED, Pam. **Sociology and the New Materialism:** Theory, Research, Action. London: SAGE Publications, 2016.

GRUSIN, Richard. Radical Mediation. **Critical Inquiry**, v. 42, n. 1, p. 124-148, 1 set. 2015.

HARMAN, Graham. **The Quadruple Object**. Winchester, UK; Washington, USA: Zero Books, 2011.

HEPP, Andreas. The communicative figurations of mediatized worlds: Mediatization research in times ofthe "mediation of everything". **European Journal of Communication**, v. 28, n. 6, p. 615-629, 1 dez. 2013.

ITU. International Telecommunication Union. **Privacy and Ubiquitous Network Societies**. Disponível em: <https://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf >, 2005.

JONES, Meg Leta. Privacy Without Screens & The Internet of Other People's Things. **Idaho Law Review**, v. 51, p. 639-660, 2015.

KARIMOVA, Gulnara Z.; SHIRKHANBEIK, Amir. Society of things: An alternative vision of Internet of things. **Cogent Social Sciences**, v. 1, n. 1, p. 1-7, 2015.

KEHR, Flavius. et al. Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. **Information Systems Journal**, v. 25, n. 6, p. 607-635, 2015.

KENNEDY, Helen; POELL, Thomas; VAN DIJCK, Jose. Data and agency. **Big Data & Society**, v. 2, n. 2, p. 1-7, 2015.

KITCHIN, Rob. Big Data, new epistemologies and paradigm shifts. **Big Data & Society**, v. 1, n. 1, p. 1-12, 2014b.

KITCHIN, Rob. **The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences**. London: Sage, 2014a.

KNIJNENBURG, Bart; KOBSA, Alfred. Increasing sharing tendency without reducing satisfaction: finding the best privacy-settings user interface for social networks. **Thirty Fifth International Conference on Information Systems**, p. 1-21, 2014.

KOKOLAKIS, Spyros. Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. **Computers and Security**, v. 64, p. 122-134, 2017.

LATOUR, Bruno. **Reassembling the Social: An Introduction to Actor-Network Theory**. Oxford: Oxford University Press, 2005.

LEMOS, André. Sensibilités Performatives. Les nouvelles sensibilités des objets dans les metrópoles contemporaines. **Revue Sociétés**, Formes In: Bruxelles: urbaines, n. 132, v. 2. p. 71-84, 2016. De Boeck, 2016.

LEMOS, André; BITENCOURT, Elias. Sensibilidade Performativa e Comunicação das Coisas: Explorando as narrativas algorítmicas na Fitbit Charge HR2. In: ENCONTRO ANUAL DA COMPÓS, 26., 2017, São Paulo. São Paulo: Faculdade Casper Líbero, 2017.

LEMOS, André; JESUS, Raniê Solarevisky de. Salvador, cidade inteligente? Comunicação e invisibilidade em experiência de IoT na capital

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

baiana. **Revista Eco-Pós**, Rio de Janeiro, v. 21, n. 3, 2017.

LENTZSCH, Christopher. et al. Integrating a Practice Perspective to Privacy by Design. In: TRYFONAS, Theo. (Ed.). **Lecture Notes in Computer Science**. Cham: Springer International Publishing, 2017. p. 691-702.

LI, Han. et al. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. **Information & Management**, v. 54, n. 8, p. 1012-1022, 2016.

LUPTON, Deborah. **Personal data practices in the age of lively data**. 2015a. Disponível em: <http://papers.ssrn.com/sol3/>. Acesso em: 03/07/2018.

LUTZ, Christoph; STRATHOFF, Pepe. Privacy Concerns and Online Behavior Not So Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses. In: BRÄNDLI, Sandra; SCHISTER, Roman; TAMO, Aurelia (Eds.), Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft [Changing multi-national companies and institutions – Challenges for economy, law, and society], pp. 81-99, Bern: Stämpfli, 2014.

MANOVICH, Lev. **Software takes command**. New York: Bloomsburry Academic, 2013.

MARTIN, Robert. The Internet of Things (IoT): Removing the Human Element. **Infosec Writers**, 2015.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data:** A Revolution That Will Transform How We Live, Work, and Think. Boston: Houghton Mifflin Harcourt, 2013.

NANSEN, Bjorn. et al. An internet of social things. **Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures the Future of Design– OzCHI '14**, v.1, n.1, p. 87-96, 2014.

O'REILLY (2005). **What Is Web 2.0?** Design Patterns and Business Models for the Next Generation of Software. Disponível em: <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>. Acesso em: 03/07/2018.

OETZEL, Marie Caroline; GONJA, Tijana. The Online Privacy Paradox: A Social Representations Perspective. **Chi 2011 Extended Abstracts on Human Factors in Computing Systems**, v.1, n.1, p. 2107–2112, 2011.

OWEN, Taylor. The violence of algorithm. **Foreign Affairs**, 2015. Disponível em: <https://www.foreignaffairs.com/articles/2015 – 05-25/violence-algorithms>.papers.cfm?abstract_id=2636709>. Acesso em: 10 jan. 2015.

PARKER, Richard B. A Definition of Privacy. **Rutgers Law Review**, v. 27, n. 2, p. 275-298, 1973.

PASQUALE, Frank. **The Black Box Society**. Cambridge: Harvard University Press, 2015.

PONCIANO, Lesandro et al. Designing for Pragmatists and Fundamentalists: Privacy Concerns and Attitudes on the Internet of Things. **Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems**, v.1, n.1. 2017.

RADFAHRER, Luli. O meio é a mediação: uma visão pós-fenomenológica da mediação datacrática. **MATRIZes,** [s.l.], v. 12, n. 1, p. 131, 2018.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

SADOWSKI, Jathan. When Data Is Capital: Datafication, Accumulation, and Extraction. **Big Data & Society**, v. 6, n. 1, p. 1-12, jan. 2019.

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s:** Redes digitais, privacidade e venda de dados pessoais. 1. ed. São Paulo: Edições Sesc SP, 2017b.

SILVEIRA, Sergio Amadeu da. Governo dos algoritmos. **Revista de Políticas Públicas**, v. 21, n. 1, p. 267, 26 jul. 2017a.

SOLOVE, Daniel. Conceptualizing privacy. **California Law Review**, v. 90, n. 4, p. 1087-1155, jul. 2002. Disponível em: <http://www.jstor.org/stable/3481326?origin=crossref>. Acesso em: 03/07/2018.

SOWE, Sulayman K.; KIMATA, Takashi; DONG, Mianxiong; ZETTSU, Koji. Managing Heterogeneous Sensor Data on a Big Data Platform: IoT Services for Data-Intensive Science. In: INT. COMPUT. SOFTW. APPL. CONF. WORK., 38, 2014. p. 295-300.

SRNICEK, Nick. **Platform Capitalism**. New Jersey: John Wiley & Sons, 2017.

TARDE, Gabriel. **A opinião e as massas.** São Paulo: Martins Fontes, 2005.

VAN DIJCK, Jose. Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. **Surveillance and Society**, v. 12, n. 2, p. 197-208, 2014.

VIANNA, Túlio. **Transparência pública, opacidade privada**. 2006. 116 f. Tese (Doutorado)–Universidade Federal do Paraná, Curitiba, 2006.

WAKEFIELD, Robin. The influence of user affect in online information disclosure. **Journal of Strategic Information Systems**, v. 22, n. 2, p. 157–174, 2013.

WESTIN, Alan. **The Origins of Modern claims to Privacy**. In: SCHOEMAN, Ferdinand David (ed.), **Philosophical Dimensions of Privacy: An Anthology**. Cambridge University Press. pp. 56-74, 1984

WILLIAMS, Meredydd; NURSE, Jason R. C.; CREESE, Sadie. The Perfect Storm: The Privacy Paradox and the Internet-of-Things. **Proceedings of 2016 11Th International Conference on Availability, Reliability and Security,** v. 1, n. 1, p. 644-652, 2016.

ZIEGELDORF, Jan Henrik; MORCHON, Oscar Garcia; WEHRLE, Klaus. Privacy in the internet of things: Threats and challenges. **Security and Communication Networks**, v. 7, n. 12, p. 2728-2742, 2014.

ZUBOFF, Shosanna. Big other: Surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, v. 30, n. 1, p. 75-89, 2015.

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611

www.e-compos.org.br
| E-ISSN 1808-2599 |

Privacy and Internet of Things: Analyzing the Nest network with Performative Sensitivity

Abstract
The relationships between privacy, technology, and communications are the main concerns in nowadays cyberculture's studies. This article aims to contribute to the debate about privacy and digital media through a critical observation of the Internet of Things. To do so, we have developed a brief review of the main aspects of Internet of Things and privacy. The concept of Performative Sensitivity will be the theoretical-methodological operator, created and used to understand the multiple dimensions of the phenomenon. As an example, we develop a quick analysis of the Nest thermostat.

Keywords
Performative sensibility. Internet of Things. Privacy. Nest.

Privacidad e Internet de las Cosas: Análisis de la red Nest con sensibilidad performativa

Resumen
Las relaciones entre privacidad, tecnología y comunicaciones son las principales preocupaciones en los estudios actuales de la cibercultura. Este artículo tiene como objetivo contribuir al debate sobre la privacidad y los medios digitales a través de una observación crítica de Internet de las Cosas. Para hacerlo, hemos desarrollado una breve revisión de los principales aspectos de Internet de las Cosas y privacidad. El concepto de sensibilidad performativa será el operador teórico-metodológico, creado y utilizado para comprender las múltiples dimensiones del fenómeno. Como ejemplo, desarrollamos un análisis rápido del termostato Nest.

Palabras clave
Sensibilidad performativa. Internet de las Cosas. Privacidad. Nest.

André Lemos
Doutorado em Sociologia pela Université René Descartes, Paris V, Sorbonne – Paris, França. Professor Titular da Faculdade de Comunicação da Universidade Federal da Bahia – UFBA, Salvador, Bahia, Brasil. Professor permanente do Programa de Pós-Graduação em Comunicação e Culturas Contemporâneas da Universidade Federal da Bahia – PPGCCC/UFBA. Pesquisador 1 A do CNPq. | E-mail: almlemos@gmail.com
ORCID: http://orcid.org/0000-0001-9291-6494

Daniel Marques
Doutorando em Comunicação e Culturas Contemporâneas pela Universidade Federal da Bahia – PPGCCC/UFBA, Salvador, Bahia, Brasil. Professor assistente da Universidade Federal do Recôncavo da Bahia – UFRB, Santo Amaro, Bahia, Brasil. | E-mail: danielmarquescontato@gmail.com
ORCID: http://orcid.org/0000-0002-7731-8581

Contribuição dos autores
Concepção e desenho do estudo: André Lemos
Aquisição, análise ou interpretação dos dados: André Lemos e Daniel Marques
Redação do manuscrito: André Lemos e Daniel Marques
Revisão crítica do conteúdo intelectual: André Lemos e Daniel Marques

E-compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), ISSN 1808-2599, v. 22, jan–dez, publicação contínua, 2019, p. 1–26. http://dx.doi.org/110.30962/ec.1611