INTERNET DAS COISAS: VULNERABILIDADE, PRIVACIDADE E PONTOS DE SEGURANÇA

INTERNET OF THINGS: VULNERABILITY, PRIVACY AND SECURITY ISSUES

André Kadow *
Carlos Eduardo Pires de Camargo **

* Mestre e doutorando em Tecnologias da Inteligência e Design Digital (PUC-SP)

** Mestre e doutorando em Tecnologias da Inteligência e Design Digital (PUC-SP)

Resumo

Este artigo visa à elaboração de uma análise sobre a maneira transparente da Internet das Coisas em nossas vidas e as possíveis implicações de segurança que ela pode trazer. Por estar presente em diversos momentos do dia a dia, muitas vezes as pessoas não percebem a quantidade de informações que são disponibilizadas e a maneira como elas serão utilizadas pelas empresas prestadoras dos serviços. Outro aspecto preocupante é se esses dados podem ser interceptados ou se os aparelhos conectados podem ser usados de outras maneiras que não a sua originalmente projetada.

Palavras-chave: Internet das coisas. Aplicativos móveis. Smartphones. Celulares. Internet.

Abstract

This article aims to draw up an analysis of the ubiquity of the Internet of Things in our future lives and the possible security implications that it can bring. Due to the fact of being present at various times of the day-to-day, people often do not realize the amount of information that is available and how they will be used by companies providing the services of Internet of Things. More worrying is that this data can be intercepted, or connected devices can be used in other ways than originally projected.

K e y w o r d s: Internet of things. Mobile app. Smartphones. cell phone. Internet.

1 Introdução

No momento em que a Internet das Coisas, *smartphones*, *tablets* e outros aparelhos conectados passam a fazer parte das nossas vidas, um futuro muito especial começa a se formar. Os campos da saúde, da engenharia, das viagens e de outras coisas mais prosaicas do nosso dia a dia estão se transformando rapidamente, trazendo-nos respostas, tecnologia e conveniência através da convergência de mídias, interfaces e dispositivos que nos apresentam respostas mais rápidas e precisas em diversos aspectos de nossas vidas. Porém essa mudança vem com um preço que merece a atenção da sociedade: a segurança. No momento em que abrimos ou conectamos os diversos momentos de nossas vidas e os disponibilizamos *online* estamos criando e compartilhando diversos dados através de redes sem fio ou de identificação por radiofrequência, também conhecida por RFID. Esse compartilhamento de informações do usuário com dispositivos, como geladeiras, pulseiras de ginástica ou brinquedos infantis, geram um perfil com diversas informações, e os mesmos aparelhos podem ajudar a alertar sobre problemas ou se adaptar melhor ao estilo de cada pessoa. Lâmpadas podem se acender no momento em que o dono da casa chega em sua residência; alimentos podem avisar quando estão para vencer, ou até mesmo alguns dispositivos podem monitorar a saúde de maneira mais intensa. Essa é a essência da *Internet das Coisas*. Uma troca constante entre usuários e aparelhos, todos conectados de alguma maneira, buscando uma vida melhor, mais fácil e mais produtiva. Tidor (2015, cap. 2) define da seguinte maneira:

> A Internet das Coisas conecta os humanos e as máquinas inteligentes de uma maneira nova, incrível e muitas vezes assustadora. Ela trata do movimento e da interação entre diversas áreas como pessoas, animais, veículos, correntes de ar, vírus e muitas outras coisas. Ela pode reconhecer relações e prever padrões muitas vezes complexos para a mente humana, pode descobrir as condições em que uma ponte se encontra, as mudanças na atmosfera. A Internet das Coisas pode ainda operar de maneira independente dos seres humanos e ficar cada vez mais inteligente com o tempo usando algoritmos adaptáveis.

Todas as benesses trazidas pela facilidade podem fazer com que os usuários não se preocupem eficientemente com sua segurança, a de sua família e dos seus dados. É que, ao compartilhar seus dados digitalmente, abre-se uma enorme via para pessoas que intencionam roubar esses dados, para falhas técnicas causadas por algum problema nos dispositivos ou ainda problema nos softwares presentes em todos os lugares, pois tais softwares ainda têm a sua origem na codificação feita por humanos e estes estão sempre sujeitos a falhas.

2 Dispositivos, Convergência e Exposição

Jenkins (2008), em seu livro *Convergence Culture,* traz um conceito que ele chama de "A falácia da caixa preta", pelo qual contesta outros autores e especialistas que defendem a ideia de um aparelho central que vai acabar cuidando e interligando diversos aspectos da vida moderna. Seria algo como uma central, a chamada caixa preta, que seria responsável pela maneira como buscamos as informações no dia a dia. Jenkins vai contra essa ideia e diz que as coisas serão encontradas em vários lugares e de diversas maneiras. Analogamente à ideia de Jenkins (2008), na Internet das Coisas as informações são capturadas, processadas e dispostas de diversas maneiras para os usuários.

Com o estilo de vida atual, em que, praticamente, todas as nossas atividades, sejam elas digitais ou físicas, são gravadas constantemente, é fundamental estabelecer o mínimo de segurança e privacidade das nossas informações. Segundo uma pesquisa realizada por Rudd (2015), um britânico tem sua imagem filmada ou fotografada mais de 300 vezes ao dia. Essa exposição a que estamos sujeitos tem várias aplicações, como em lojas ou supermercados – que, através do reconhecimento facial ou por outro meio conseguem personalizar ofertas e produtos para determinados clientes –, mas também abrem espaço para pessoas mal-intencionadas capturarem os seus dados e depois os utilizarem de maneiras escusas.

Tecnicamente falando, um dos possíveis elementos facilitadores àqueles que querem se aproveitar ilicitamente da Internet das Coisas é a maneira como muitos dos dispositivos são programados. O desenvolvimento através de Application Programming Interface - APIs ou linguagem comuns é um enorme facilitador para os fabricantes e desenvolvedores, mas abre um leque enorme de

possíveis brechas a serem exploradas. Em um mundo com aparelhos conectados com seus próprios endereços IPs ou outros identificadores necessários para a comunicação entre usuário e máquina, o campo para ataques acaba se tornando imenso. Mesmo com as linguagens comuns, para os administradores é praticamente impossível garantir a segurança de todos os aparelhos conectados e as ações funcionam cada vez mais da maneira que os fabricantes de antivírus para computadores trabalham, as soluções vão ocorrendo na medida em que os problemas vão aparecendo e não da maneira contrária.

Com todas essas mudanças, interações feitas cada vez mais por sistemas inteligentes no lugar de humanos, a tendência a erros por distração ou esquecimento estão ficando cada vez mais longe. Um ponto interessante é notar que, sem a Internet das Coisas, estamos passíveis de mais erros, mas teoricamente em menor escala e com a mesma, a quantidade de erros, teoricamente, deve ser menor mas com um agravante de maior escala dada a sua penetração. Como analisado por Tidor (2015), o grande desafio das tecnologias é desenvolver um grau de confiança e segurança. Enquanto elas removem os fatores humanos das tomadas de decisões como julgamentos errados, ela introduz um novo problema que é trocar acidentes menores por outros em maior escala. É o chamado paradoxo da automação. Enquanto as chances de acidentes diminuem, as consequências aumentam exponencialmente.

Podemos citar como exemplo a fábrica de turbinas de avião da Rolls Royce, onde é possível monitorar em tempo real todas as turbinas fabricadas pela empresa, se estão em funcionamento ou não, observar a telemetria, em que avião estão instaladas e em que lugar do globo terrestre esse avião está. Em um exemplo hipotético, se por uma falha de software ou mesmo a invasão de um *hacker* dentro desse sistema fizesse todas as turbinas se desligarem, teríamos um acidente de proporções épicas.

Outro problema não tão trágico, mas também complexo, que a Internet das Coisas pode nos trazer é a perda de privacidade. Dispositivos podem capturar todos os hábitos de consumo de alguém, e as empresas donas desses dispositivos podem usar esses dados para criar um perfil detalhado sem que o consumidor saiba.

Ainda mais complicado são os dispositivos de imersão, como o Kinect do videogame *Xbox One* da Microsoft, ou outros similares, que permitiriam às

empresas um mapeamento constante das pessoas. Através desses dispositivos, aos quais ficamos conectados jogando, abrimos uma janela para as empresas sobre o que consumimos, o estilo de nossa casa, de nossas roupas etc., afinal para existir a interação, o aparelho faz a captura da pessoa e de todos os outros objetos presentes no local. Assim é possível, através de softwares de reconhecimento, verificar se alguém consome a marca X de refrigerante no lugar da Y, se joga com mais pessoas e, dessa maneira, criar um perfil preciso dos seus consumidores e impactá-los de maneira mais eficiente. Outra aplicação seria também o monitoramento para fins governamentais ou mesmo de espionagem, servindo como um complemento dos sistemas já existentes. Esse tipo de preocupação é tão real, que a própria Microsoft se manifestou publicamente, em 2013, através do vice-presidente da divisão de entretenimento Phil Harrison, em uma entrevista para o jornalista Tom Bramwell, de acordo com Eurogamer.Net (2013) que não compartilha os dados com nenhuma outra empresa e nem com o governo americano.

Um problema semelhante foi levantado por Harris (2016), ao afirmar que as *smartTVs* da marca Samsung também capturam e transmitem tudo o que as pessoas falam em frente aos aparelhos caso a opção de comando por voz esteja ativada; o fato foi confirmado pela fabricante coreana.

Outros exemplos são o de Greenberg (2015), segundo o qual *hackers* conseguiram desligar os freios de um Corvette em pleno movimento usando um simples dispositivo e um celular; ou também da preocupação de Gornall (2015) a respeito dos marca-passo ou outros dispositivos cardíacos, que segundo ele, por estarem conectados à rede para facilitar o acompanhamento da família e dos médicos também colocam a vida do paciente nas mãos de outros.

3 New Deal dos Dados ou Transparência Total?

Diante de tantas questões sobre segurança e privacidade que surgem com o advento da Internet das Coisas, pesquisadores, cientistas e outros interessados começam a vislumbrar possíveis caminhos. Do MIT Media Lab, Pentland (2014) propõe um conjunto de princípios e práticas para definir a propriedade dos dados e controlar seu fluxo. Apesar de levar em conta os interesses dos principais *stakeholders* – usuários, empresas e governos – esta proposta busca um

reequilíbrio da propriedade de dados em favor do indivíduo cujos dados são coletados. Ele chama a este conjunto de regras de *New Deal* dos dados em referência à série de programas implementados por Franklin Roosevelt nos EUA, após a crise econômica de 1929, com o objetivo de reformar a economia americana.

A base dessa proposta é a transparência. O *New Deal* dos dados daria às pessoas a capacidade de ver o que está sendo coletado sobre elas e, assim, poderiam optar em aceitar ou não tal coleta. Se, por um lado, o monitoramento dos padrões da vida de uma pessoa pode permitir um alto grau de personalização de remédios, seguros, entretenimento, dentre tantos outros produtos e serviços, por outro, o que seria do cidadão se esses mesmos dados fossem gerenciados de maneira integral e exclusiva pelas grandes corporações? Por questões como essa, Pentland (2014) declara preferir que o retrato completo do indivíduo seja de propriedade do próprio indivíduo e, mesmo que em alguns casos, essa regulamentação possa inviabilizar alguns modelos de negócios, a transparência deve tornar a economia mais saudável.

O que Pentland (2014) propõe com o *New Deal* dos dados é que as empresas terão de informar claramente aos seus clientes quais dados serão coletados e como os utilizarão, e a palavra final em aceitar ou não essa condição caberá exclusivamente ao cliente. Ou seja, as empresas terão de convencer os consumidores dos benefícios que terão em troca dos seus padrões de dados; mas há também vantagens para as empresas. Sem essa transparência, elas assumem enormes custos e riscos com uma política de obtenção de todos os dados irrestritamente. Nas palavras de Pentland (2014, p. 85 - 88):

> Acho que as empresas não percebem que os custos de uma estratégia do tipo 'pegue todos os dados' são muito altos. Elas estão assumindo enormes quantidades de risco na forma de violações de dados e danos a sistemas essenciais. Além de ser caro manter a segurança, as violações custarão cada vez mais caro. A Comissão Federal de Comércio dos EUA já deixou bem claro que agirá duramente. Além do risco financeiro, existe o risco para a marca.

Em resumo, o *New Deal* dos dados não proíbe as empresas de criar produtos rentáveis a partir dos dados de seus clientes, apenas determina que suas regras

e princípios de transparência devem ser respeitados. Ainda segundo Pentland (2014), em Trento, na Itália, centenas de famílias estão vivendo experimentalmente sob o *New Deal* dos dados, recebendo notificações e controle sobre os dados gerados por elas, e esses dados são compartilhados e auditados. O resultado medido até agora aponta para o fato de que essas pessoas têm a tendência de compartilhar muito mais do que as que não vivem sob esse regime.

Kranenburg (2008) apresenta outro ponto de vista sobre como dar conta das questões de privacidade e segurança em tempos de Internet das Coisas. Para ele, a solução tem caráter mais idealista, em contraste com o senso prático de Pentland (2014), mas a questão da transparência permanece. Para o holandês:

> [...] um bem comum maior pode ser estabelecido se a vigilância for igual para todos e se o público tiver o mesmo acesso [aos dados] de quem está no poder, por isso, defendemos que seria bom para a sociedade se a arquitetura da 'Internet das Coisas' fosse igual para todos, e o público tivesse as mesmas ferramentas dos que estão no poder (KRANEMBURG, 2008, p. 9).

Sua proposta é a de uma transparência radical. Nela todos os dados seriam públicos, dados pessoais, empresariais, governamentais etc. E todos teriam acesso a tudo. Se as empresas e governos podem tomar decisões baseadas nos padrões de comportamento, saúde e consumo dos seus clientes e cidadãos respectivamente, os indivíduos teriam também o mesmo poder de acesso a todos os dados corporativos, dos mais óbvios aos mais sigilosos, e poderiam interferir de forma mais efetiva nas diretrizes empresariais e governamentais. Isto, segundo Kranemburg (2008), deixaria todos os *stakeholders* em pé de igualdade.

Da Holanda de Rob van Kranemburg chegam as notícias da implementação de um sistema de Internet das Coisas construído sob a ideologia da transparência e liberdade de uso: trata-se do projeto *The Things Network* (2015). Construída pelos próprios cidadãos de Amsterdam, esta rede, baseada na tecnologia *LoraWan* [TD] , cobriu todo o perímetro urbano de Amsterdam em apenas seis meses, e começa a se espalhar pelo mundo. Cidades como Boston, Montevideo, Zurique e mesmo São Paulo já se movimentam na mesma direção. Segundo a declaração de visão do projeto *The Network of Things (2015,)*:

> A internet foi criada por pessoas que conectaram suas redes e permitiram gratuitamente o tráfico através, para e sobre seus servidores e cabos. Como resultado, houve abundante comunicação de dados e inovação exponencial. A *Things Network* está fazendo o mesmo pela Internet das Coisas através da criação de abundante conectividade de dados. Assim, aplicações e negócios podem florescer.

4 Conclusão

Com a Internet das Coisas, novas e interessantes possibilidades de desenvolvimentos tecnológicos apresentam-se à sociedade. A vida e a convivência humana podem ser muito beneficiadas, mas importantes questões de segurança têm de ser levadas em conta. De certo modo, essas questões relacionam-se diretamente à propriedade e guarda dos dados gerados pelos dispositivos inteligentes e conectados. Quem são os proprietários desses dados, as empresas que os coletam ou os usuários? Quem os gerencia e garante sua integridade? Quem os protege da ação de agentes mal-intencionados?

Segundo Santaella (2013) o governo da privacidade e, consequentemente, da segurança está sempre sob o ataque de interesses públicos e privados poderosos, prontos para usar as novas tecnologias da informação em nome da administração de risco para esconder a acumulação de lucros. Por outro lado, ataques de agentes mal-intencionados também podem afetar de maneira prejudicial o ambiente da Internet das Coisas, através de ataques de *hackers* isolados ou grupos de ação ligados ao terrorismo digital e outros *cibercrimes*. Desta forma, a ponta mais frágil do sistema acaba sendo o indivíduo que, ao usufruir das novas possibilidades tecnológicas, coloca-se à mercê de grupos mais poderosos.

Assim, iniciativas como o *New Deal* dos dados, de Pentland (2014), e a transparência total de Kranemburg (2008), que consideram o respeito ao indivíduo como principal fator a ser considerado no fluxo, na coleta, na armazenagem e no gerenciamento de dados pelos *stackeholders* mais poderosos são bem-vindas. Mas, com certeza, ainda estamos distantes de uma solução satisfatoriamente eficiente para a segurança da avalanche de dados que, cada vez mais, é deixada como rastro digital do uso da rede.

Referências

EUROGAMER.NET. *The big interview*: Phil Harrison on Xbox One, Kinect, indie games and red rings. 2013. Disponível em: <http://www.eurogamer.net/articles/2013-05-21-phil-harrison-on-xbox-one-kinect-indie-games-and-red-rings>. Acesso em: 14 fev. 2016.

GORNALL, Jonathan. *The heart pacemakers at risk from hackers*: sound far-fetched? Security experts are treating it deadly seriously. 2015. Disponível em: <http://www.dailymail.co.uk/health/article-3252609/The-heart-pacemakers-risk-hackers-Sound-far-fetched-Security-experts-treating-deadly-seriously.html>. Acesso em: 04 nov. 2015.

GREENBERG, Andy. *Hackers cut a corvette's brakes via a common car gadget.* 2015. Disponível em: < http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via--common-car-gadget/>. Acesso em: 4 nov. 2015.

HARRIS, Shane. Your Samsung smarttv is spying on you, basically.*The Daily Beast,* [S.L], fev. 2015. Disponível em: <http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html>. Acesso em: 13 fev. 2016.

JENKINS, Henry. *Convergence culture:* where old and new media collide. New York : NYU Press, 2008.

KRANENBURG, Rob van. *The internet of things*: a critique of ambient technology and the all-seeing network of RFID. Amsterdam: Institute of Network Cultures, 2008.

PENTLAND, Alex. Com os grandes dados vêm grandes responsabilidades. *Harvard Business Review Brasil*, São Paulo, v. 92, n. 11, nov. 2014.

RUDD, Matt. Say cheese. *The Sunday Times***,** Londres, jun. 2015. Disponível em: <http://www.thesundaytimes.co.uk/sto/Magazine/article1566128.ece>. Acesso em: 13 fev. 2016.

SANTAELLA, Lucia. *Comunicação ubíqua:* repercussão na cultura e na educação. São Paulo: Paulus, 2013.

The Things Network (2015). Our Vision. Disponível em <http://www.thethingsnetwork.org> Acesso em 30 de nov. 2015.

TIDOR, Bruce. *The internet of things.* Oxford: The MIT Press, 2015.