Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 282-290
ISSN 1679-1827
http://www.revista.ufpe.br/gestaoorg

O Desafio da Privacidade na Internet das Coisas

The challenge of privacy on the Internet of things

Carlos Cesar Santos[1], Jefferson David de Araújo Sales[1]

[1]Universidade Federal de Sergipe, UFS, Brasil

Correspondência: Carlos Cesar Santos, Endereço: Av. Marechal Rondon, Cidade Universitária Prof. Aloísio de Campos, Jardim Rosa Elze, CEP.: 49.100-000 São Cristovão, Brasil. Tel.: 55 79 2105-6944 E-mail: cordcesar@hotmail.com

Recebido: 14 de outubro de 2015 Aceito: 26 de março de 2016 Publicado: 09 de maio de 2016

Resumo

Na ultima década a internet tornou-se uma ferramenta presente no cotidiano das pessoas e das organizações e por vez indispensável ao bom funcionamento dos negócios. Com o crescente incremento das infraestruturas de redes e popularização em massa da rede de alta velocidade, emerge um avanço relacionado à utilização da internet tornando-a uma plataforma global para deixar máquinas e objetos inteligentes capazes de comunicarem-se de forma autônoma. Esta possibilidade permite que conteúdos e serviços estejam em torno das pessoas, sempre disponíveis, facilitando a comunicação e abrindo o caminho para novas aplicações, possibilitando novas formas de trabalho, de interação e de entretenimento, fazendo com que um novo padrão de vida e de trabalho seja desenvolvido. Este novo padrão torna-se possível através dos avanços das Tecnologias da Informação e Comunicação - TICs até uma nova concepção definida como *Internet of Things* - IoT. Entretanto, com uma variada coleta de dados e informações, para variados fins, no cotidiano das pessoas e das organizações, a coleta autônoma dos dados e das informações torna a privacidade um dos principais desafios em relação à IoT. Neste contexto, este artigo objetiva discutir em âmbito teórico a privacidade dos usuários da tecnologias da Internet das Coisas, diante de sua legalidade, explorando possíveis soluções neste cenário ainda em construção.

Palavras-chave: Internet das Coisas; Privacidade; Segurança da Informação

Abstract

In the last decade the Internet has become a tool in this everyday people and organizations and time essential to the smooth operation of businesses. With the increasing development of infrastructure networks and mass popularization of the high-speed network, emerges a related Internet use forward making it a global platform to make intelligent machines and objects able to communicate up autonomously. This possibility enables content and services are around people, always available, facilitating communication and paving the way for new applications, enabling new forms of work, interaction and entertainment, making a new pattern of living and working is developed. This new standard is made possible through advances in Information and Communication Technologies - ICTs to a new concept defined as Internet of Things - IoT. However, with a varied collection of data and information for various purposes in the daily lives of people and organizations, autonomous data collection and information makes privacy a major challenge regarding the IoT. In this context, this article aims to discuss theoretical framework the privacy of users of the Internet of Things technologies in front of their legality, exploring possible solutions in this scenario still under construction.

Keywords: Internet of Things; privacy; Information security

1. Introdução

Cerca de dois bilhões de pessoas ao redor do mundo usam a Internet para se comunicar, navegar na Web, acessar conteúdos e serviços multimídia, jogos, interagir em redes sociais e muitas outras aplicações. Com o crescente incremento das infra-estruturas de redes e popularização em massa da internet de alta velocidade, emerge um avanço relacionado à utilização da internet tornando-a uma plataforma global para deixar máquinas e objetos inteligentes capazes de comunicarem-se de forma autônoma (MIORANDI et al., 2012).

Gao e Bai (2014) destacam que durante a próxima década, a rede inter-existirá como um tecido sem costura de redes clássicas e objetos ligados em rede. O conteúdo e serviços estarão em torno das pessoas, sempre disponível, facilitando a comunicação e abrindo o caminho para novas aplicações, possibilitando novas formas

de trabalho, de interação, de entretenimento, fazendo com que um novo padrão de vida seja desenvolvido. Este novo padrão de vida, torna-se possível através dos avanços das TICs até uma nova concepção definida como *Internet of Things* - IoT.

O termo *Internet of Things* foi cunhado pela primeira vez em 1999 por Ashton, um dos pioneiros da tecnologia britânica que ajudou a desenvolver o conceito (GUBBI et al., 2013). A IoT visa estender os benefícios da internet proporcionando uma conectividade constante, desenvolvendo uma capacidade de controle remoto e compartilhamento de dados para os bens no mundo físico (PEOPLES et al., 2013).

A Internet das Coisas - IoT advém do conceito de presença generalizada em torno das pessoas e de uma variedade de coisas ou objetos, através de *Radio Frequency IDentification* - RFID, sensores, atuadores, *gadget* como *smartphones*, *tablet*, televisores, pulseiras e relógios inteligentes, etc., por meio de esquemas de endereçamento exclusivos que são capazes de interagir uns com os outros e cooperar com os seus vizinhos para alcançar objetivos comuns (ATZORI; IERA; MORABITO, 2010).

Dentro dessa perspectiva, o termo *Internet of Things* - IoT é amplamente usado para se referir a ambos: A rede global resultante da interligação dos objetos inteligentes; Ao conjunto de tecnologias de apoio necessárias para concretizar essa visão; E o conjunto de aplicações e serviços que alavancam tais tecnologias para abrir novas oportunidades de negócios e de mercados (MIORANDI et al., 2012).

A eficácia da IoT reside no alto impacto que ela se dispõe a proporcionar sobre diversos aspectos do cotidiano de vida e comportamento de usuários potenciais (PEOPLES et al., 2013). Do ponto de vista de um usuário privado, os efeitos mais evidentes da introdução da IoT estão em suas funções assistidas, como em cuidados com a saúde, orientação de aprendizagem e controle doméstico, são apenas alguns exemplos dos campos de aplicação da IoT. Da mesma forma, a partir da perspectiva dos usuários de negócios, as consequências mais aparentes serão igualmente visíveis em áreas como automação e manufatura industrial, logística, processo de gestão e tomada de decisão, transporte inteligente de pessoas e bens (ATZORI; IERA; MORABITO, 2010).

Com uma variada coleta de dados e informações, para variados fins, no cotidiano das pessoas, seja em ambientes domésticos de usuários privados ou em ambientes profissionais de usuários de negócios, a coleta autônoma dos dados e das informações das pessoas torna a privacidade uma das principais preocupações éticas com relação à Internet das Coisas. Intendida por Chabridon et al. (2014) como uma questão crucial que pode limitar a implantação da visão IoT seja para usuários privados ou para organizações.

Chabrindon et al. (2014) e Weber e Weber (2010) ressaltam que a privacidade é fundamental para o controle deste novo ambiente complexo. A troca de dados invisível e constante entre as coisas e as pessoas, e entre as coisas e outras coisas, irá ocorrer de forma que os proprietários e criadores desses dados não sejam identificados. A própria escala e capacidade das novas tecnologias vai ampliar este problema.

O termo privacidade transmite um grande número de conceitos e ideias. Comumente associa-se privacidade com a noção de um indivíduo que controla o acesso a sua informação pessoal. Weber e Weber (2010) identificam três áreas relacionadas com a privacidade, sendo elas: O espaço físico, que pode ser compreendido como um escudo contra objetos indesejados ou sinais, neste sentido a privacidade está perto de segurança de infra-estrutura; O poder de tomada de decisão em relação ao fluxo de informações com o objetivo de proteger a liberdade de uma pessoa a fazer escolhas a respeito de seus dados; E o controle de um indivíduo sobre o processamento da informação compreendendo a aquisição, divulgação e uso de informações pessoais.

No entanto, Chabrindon et al. (2014) afirmam que preservar a privacidade através do isolamento não é mais uma opção no mundo da informação e da comunicação de hoje. Para um contexto de ambiente inteligente gerado pela Internet das Coisas, onde as aplicações tornassem de fácil usabilidade e as informações são disponibilizadas de maneira muitas vezes imperceptíveis, a privacidade é geralmente percebida pelos usuários como uma expectativa de estar em um estado de proteção sem ter que persegui-lo ativamente.

Nessa linha, Marx e Murky (2001) identificaram quatro níveis de privacidade percebíveis pelas pessoas, estes níveis são posteriormente destacados por Chabrindon et al. (2014) para definir a maneira como as pessoas percebem as violações a sua privacidade, sendo estes níveis nomeados como fronteiras: A fronteira natural impede a sua presença (ou sentimentos ou emoção) de ser percebido através de um dos sentidos humanos, como paredes, portas, cartas seladas, telefone e email representam fronteiras naturais para observação; A fronteira da sociedade envolve expectativas das pessoas para certos papéis sociais (médicos, membros do clero, advogados) profissionais que não vão divulgar informações confidenciais; A fronteira espacial ou temporal que separa a informação dos vários períodos ou aspectos da vida da pessoa; E a fronteira dos efeitos efêmeros ou transitórios, tais fronteiras baseiam-se na ideia de que a interação e comunicação são esquecidas em breve.

Nota-se que a IoT, enquanto inovação tecnológica que envolve questões de privacidade de dados e informações de usuários, ganha espaço nas discussões acaloradas em meios acadêmicos e profissionais. Assim, com vistas a contribuir para amplificação das discussões este texto visa discutir, de modo conceitual, os mais relevantes elementos que compõem o fenômeno da IoT. Para isso, o escrito divide-se em cinco sessões: esta introdução

como primeira etapa; três sessões teóricas que versam sobre a origem da internet das coisas; privacidade e a IoT; e perspectivas legais da privacidade da informação. E, por fim, são feitas as considerações finais na tentativa de fomentar novas propostas de estudo.

2. Origem da Internet das Coisas

Ao longo de seus primeiros 40 anos, a Internet tem sido usada principalmente para conectar pessoas através de troca de e-mails, fóruns de discussão e, cada vez mais, por meio de sites de redes sociais que coletam e distribuem dados e informações. Também nota-se que na atualidade a Internet é utilizada para conectar dispositivos, máquinas e outros objetos, através de redes com e sem fio, criando um novo posicionamento tecnológico nomeado de *Internet of Things* (DUTTON, 2014).

A *Internet of Things*, ou Internet das Coisas, como é chamada em português, ganhou uso pela primeira vez em 1999 por Ashton (2009), um dos autores pioneiros nesse tipo de tecnologia, cuja as pesquisas ajudaram a desenvolver o conceito atual desse posicionamento tecnológico.

A IoT, visa estender a capacidade de conectividade constante de compartilhamento de dados, o controle a distância, dentre outras capacidades para o mundo físico (PEOPLES, 2013). Permitindo que objetos físicos armazenem, enviem e recebam informações de maneira que possam transformar a forma como as pessoas fazem as coisas e justificar a Internet das Coisas como um novo conceito tecnológico (DUTTON, 2014).

Neste contexto Li, Da Xu e Zhao (2014) que define a IoT como um conjunto de aplicações habilitados para a Internet com base em objetos físicos e o meio ambiente integrando aos da rede de informação. A IoT consiste nos protocolos e tecnologias relacionadas que permitem que elementos diferentes se comuniquem através de canais de comunicações eletrônicas, com ou sem fio, numa rede de troca de dados e informações compostas por coisas e pessoas (VALÉRY, 2012). Logo, como salienta Dutton (2014) a IoT destaca-se por permitir que informações eletrônicas passem a ser transmitidas por objetos físicos, como quando eles se movem através do espaço, de forma semelhante a redes sem fios que transmitem sinais eletrônicos, criando uma verdadeira nova dimensão para a concepção e utilização da Internet.

A próxima grande inovação da sociedade moderna será a plena implementação da Internet das Coisas, conectar não apenas as pessoas, mas também as máquinas, coisas e objetos inteligentes, graças à conectividade sem fio (DUTTON, 2014). A comunicação entre coisas e pessoas será possível independentemente das circunstâncias de local e de forma, apresentando um novo posicionamento tecnológico na comunicação moderna (ROMAN; NAJERA; LOPEZ, 2011). Possibilitado por uma variedade de dispositivos conectados e identificados, torna-se possível perceber eventos e alterações dentro do chamado ambiente inteligente (CHABRIDON, *et al*., 2014).

O impacto social e organizacional que a IoT potencialmente provoca na utilização das TIC's pode reconfigurar a maneira como as pessoas lidam com as informações, como convivem, como recebem e fornecem serviços e como utilizam as tecnologias existentes (PANG et al., 2015). Esperar que tais inovações pautadas na Internet das Coisas aconteçam justifica-se por uma série de características, sendo em primeiro lugar a flexibilidade que a IoT apresenta, sustentada pelas variadas combinações de tecnologias e soluções que podem ser aplicadas de variadas maneiras e adequadas a variados contextos, além dos constantes aperfeiçoamentos pelos quais componentes chaves da IoT passam para ampliar sua capacidade, vida útil e escala de produção de maneira a possibilitar novas áreas de aplicação em potencial (DUTTON, 2014).

Segundo, é importante destacar que a IoT nem sempre faz algo inteiramente novo, mas faz as coisas mais próximas em tempo real e em um maior nível de precisão do que já foi feito antes. Em terceiro lugar, a IoT posiciona a partilha de dados no epicentro da sua aplicabilidade, tornando essencial a integração dos dados em diferentes setores e serviços já existentes e que venha a serem criados no futuro (DUTTON, 2014; ASHRAF; HABAEBI, 2015).

Entretanto, a ideia de compartilhar dados coletados para um propósito afim de apoiar outro propósito distinto está repleto de novas questões de ordem ética, de ordem política e de ordem prática, mas a ideia de compartilhamento é fundamental para permitir que a IoT seja capaz de suportar aplicações que envolvem o conhecimento do comportamento. Combinar os dados de diferentes indivíduos torna-se a chave para o pleno funcionamento da IoT, contudo gera um desafio recorrente ainda maior em relação a privacidade dos seus usuários (DUTTON, 2014).

3. Privacidade e a IoT

A privacidade é uma das principais preocupações éticas dos usuários com relação à Internet das Coisas e é uma questão crucial que pode limitar a implementação da visão IoT (MIORANDI et al., 2012). O controle deste novo ambiente complexo, a troca de dados invisível e constante entre as coisas e as pessoas, e entre as coisas e outras coisas, precisa ocorrer de maneira anônima, sem o conhecimento dos proprietários e criadores desses dados. A própria escala e capacidade das novas tecnologias vai ampliar este problema. Controlar os dados recolhidos por todos os objetos conectados que compõem o ambiente inteligente torna-se uma tarefa chave para o

desenvolvimento dessa nova realidade (CHABRIDON et al., 2014).

Krause e Hochstatter (2005) apontam a privacidade como o direito de ser deixado em paz. Por seu turno, Krause (2009) afirma que preservar a privacidade através do isolamento não é mais uma opção no mundo da informação e da comunicação existente no século XXI. Segundo Chabridon et al. (2014) a privacidade é agora geralmente percebida pelos usuários como uma expectativa de permanecer num estado de proteção sem ter que persegui-lo ativamente. Os usuários só demonstram preocupação efetiva com a privacidade quando sentem que esta foi violada. Marx (2001) identifica quatro linhas de fronteira pessoais que são percebidas como violações de privacidade, sendo estas apresentadas a seguir no quadro 1

Quadro 1: Linhas de fronteiras pessoais

Linha de fronteira	Descrição
A fronteira natural	Impede a presença, sentimentos e/ou emoções não sendo percebidos através dos sentidos humanos. Paredes, portas, roupas, escuridão, cartas seladas, telefone e email representam fronteiras naturais para observação.
A fronteira social	Envolve expectativas que as pessoas com certos papéis sociais como médicos, membros do clero, advogados e outros não irão divulgar informações confidenciais a eles fornecidas pelas pessoas envolvidas.
A fronteira espacial ou temporal	Separa a informação dos vários períodos ou aspectos da vida da pessoa.
A fronteira dos efeitos transitórios	Supõem que a interação e a comunicação são efêmeros e transitórios como ações que se esperam, sendo facilmente esquecidas em um curto espaço de tempo.

Fonte: Baseado em Marx (2001).

Solove (2006) argumenta que nenhuma definição de privacidade é capaz de atender a todos os aspectos compreendidos pela privacidade, mas sim que existem várias formas de privacidade, propondo uma taxonomia de privacidade com uma visão geral das atividades que possam levar a sua violação, sendo elas:

- A coleta de informações, que embora a informação geralmente seja recolhida com o consentimento do proprietário da informação, cobranças forçadas ou interrogatórios podem levar a violação da privacidade da pessoa.
- A disseminação da informação, quando realizada pode de incorrer no estrapolamento da confidencialidade, podendo tal situação ser gerada de múltiplas formas.
- A divulgação pode acontecer com a publicação de fatos verídicos, no entanto, tais fatos podem afetar a reputação da pessoa, por meio da exposição de dados e informações privados que possam vir a serem vinculados.
- E a invasão que pode ocorrer nos dados pessoais por meio do acesso intrusivo em sua pessoalidade e através da interferência decisória.

Como foi assinalado por Krause (2009), embora esta taxonomia pretende ser utilizada para proteção legal, poderá também ser útil para as tecnologias. Os fornecedores de tecnologia devem analisar sistematicamente se algum *software* ou tecnologia pode aumentar as chances de tal problema ocorrer, e buscar desenvolver soluções que possam mitigar tais chances (CHABRIDON et al., 2014).

Chabridon et al. (2014) baseados nos estudos de Danezis e Gurses (2010) categorizam aspectos de privacidade em três classes distintas, sendo elas a privacidade como confidencialidade, a privacidade como controle e a privacidade como transparência, cada categoria com distinções entre si, como apresentado a seguir.

A privacidade como confidencialidade é normalmente presente de alguma forma em tecnologias existente, com o primeiro objetivo é proteger a privacidade dos dados pessoais evitando que estes sejam acessados por pessoas não autorizadas. Se os dados pessoais se tornam públicos, a confidencialidade e privacidade, portanto, são perdidas. Privacidade como confidencialidade representa as soluções para garantir o anonimato dos dados, das comunicações (SAXBY, 2015).

A abordagem anonimato parte da ideia de que o indivíduo não pode ser identificado dentro de um conjunto de usuários. No entanto, o grau de anonimato considerado suficiente em um caso específico de uso particular depende diretamente de consequências legais e sociais causadas por uma possível violação de dados e ainda é uma questão em aberto como destacam Chabridon et al. (2014). Diferencial de privacidade tem como objetivo

fornecer meios para maximizar a precisão das consultas a partir de bases de dados estatísticos, minimizando as chances de identificar os seus registos **(**VAIDYA, 2012).

A geração desse anonimato nas comunicações visa proteger os dados de tráfego e esconder quem fala com quem na rede. Mesmo que o conteúdo de uma comunicação seja mantido em sigilo, informações confidenciais podem ser vazadas por dados de tráfego que incluem locais e as identidades das partes em comunicação, tempo, frequência e volume da comunicação. Por isto, fornecer comunicação anônima é um desafio uma vez que muitos protocolos de comunicação usam identificadores únicos (MATOS; 2012; VAIDYA, 2012).

A abordagem da privacidade como controle refere-se à capacidade de controlar o que acontece com os dados pessoais para evitar abusos por parte de terceiros. Isto requerer tecnologias para a especificação e aplicação de políticas de privacidade. Para direcionar estes aspectos de controle, Wang e Kobsa (2008) identificam 11 princípios fundamentais da privacidade, com apresentado no quadro 2.

Quadro 2: Onze princípios fundamentais da privacidade

Princípio	Descrição
A consciência de utilização	Baseada em declarações claras e bem detalhadas das políticas de privacidade.
A minimização dos dados	Busca avaliar a necessidade, eficácia e proporcionalidade de novas tecnologias antes de sua implantação, dando preferência a soluções menos invasivas.
A especificação de objetivos	Observa a finalidade para qual os dados estão sendo coletados.
A limitação de coleta	Objetiva definir os limites para a coleta de dados a ser realizada.
A limitação de uso	Defini-se a fim de evitar que dados sejam usados ou divulgados para fins que não tenham sido especificados no momento da coleta.
A proteção de transferência	Deve ser definida para evitar que dados sejam transferidos caso a garantia de proteção adequada não possa ser mantida.
A capacidade de escolha e consentimento	Baseia-se no princípio de que os indivíduos devem possuir a capacidade de decidir sobre a coleta, uso e divulgação de seus dados.
O acesso	Garante que as pessoas podem verificar seus dados armazenados.
A integridade	Princípio base para garantir que os dados recolhidos serão destinados para a finalidade a que se destinam.
A segurança	Garantia de que os dados estão fora de risco de perda, acesso não autorizado, uso indevido, modificação ou divulgação não autorizada.
A aplicação	Preocupa-se diretamente com a existência de mecanismos que façam cumprir princípios de privacidade.

Fonte: Baseado em Wang e Kobsa (2008).

Na sequência, a abordagem da privacidade como transparência pretende aprimorar a compreensão das pessoas e seu controle sobre os dados que são coletados, tal pretensão traduz-se na aplicação de quatro características definidas por Castellucia et al. (2011) como cruciais para que essa tecnologia alcance a transparência, sendo elas:

- A capacidade de fornecer informações sobre a coleta, destinação, armazenamento e processamento dos dados;
- A capacidade de fornecer relatórios capazes de informar quais dados foram divulgados, para quais finalidades e sobre o abrigo de quais políticas;
- A capacidade de proporcionar acesso *on-line* pelos seus proprietários aos dados; e

- A capacidade de ajudar o usuário a prever possíveis oportunidades e riscos relevantes a sua privacidade.

Privacidade como a transparência é uma questão importante porque a maioria das tecnologias são inúteis se as pessoas não podem usá-los de forma eficiente. Privacidade como a transparência é ainda mais crítico para os sistemas distribuídos baseados na IoT do que as aplicações onipresentes baseados na *web* existentes. Os usuários, não só terão que controlar os dados pessoais que podem ser propagados a partir dos terminais com os quais eles interagem diretamente, como smartphone e tablets, mas também terão que lidar com o controle dos dados produzidos automaticamente pelas coisas conectadas que eles possuem, que os cercam ou que estão localizados em ambientes que frequentam como shopping, escritórios, consultórios e etc (VAIDYA, 2012; SAXBY, 2015).

Vislumbrando a complexa relação da privacidade com o usurário algumas abordagens tentam envolver os utilizadores na gestão da privacidade, propondo a melhoraria da compreensão dos usuários a respeito das implicações de privacidade, fornecendo-lhes *feedback*, relatórios de privacidade para permitirem que os usuários definam seus controles primários e, em seguida, verifiquem a forma como os seus dados privados são vistos a partir do ponto de vista das outras pessoas (CHABRIDON et al., 2014).

No entanto Weber e Weber (2010) salientam que a preocupação com a privacidade das informações faz com que o risco de um controle rigoroso por parte do proprietário, possa colocar em risco a veracidade de certas atividades, ocultando informações que possam vir a indicar determinadas atividades criminosas. Neste sentido a privacidade das informações pode, a longo prazo, não ser necessariamente indissolúvel portanto, o quadro jurídico deve ser elaborado para lidar com esse fenômeno precisa está adaptado a está nova realidade. Na próxima sessão será apresentado um panorama geral das principais iniciativas legislativas em relação a privacidade.

4. Perspetivas Legais da Privacidade da Informação

Conceber as inovações transformadoras que a Internet das Coisas potencialmente pode gerar sem refletir sobre os riscos sociais, éticos e legais que as envolvem torna-se inexequível quando trata-se de aplicações que possibilitam o controle, a localização, o monitoramento da saúde das pessoas entre outras variadas possibilidades. A maioria das preocupações centralizam-se nos riscos de comprometer a privacidade pessoal de um indivíduo, criando sistemas que tornam a protecção de dados cada vez mais crítico ao abrigo do direito e das leis existentes (DUTTON, 2014).

Privacidade e vigilância estão entre uma série de riscos sociais e éticos ligados à Internet das Coisas (SPIEKERMANN, 2013). A população de grandes metrópoles já são monitoradas diariamente por câmeras de vigilância e o advento da IoT tem a capacidade de alargar ainda mais esse potencial de vigilância, pública e privada levando-a a locais ainda não alcançados pela indústria de segurança tradicional (WEBER; WEBER, 2010).

Tal expectativa demonstra que as questões de privacidade são difíceis de resolver e tendem a tornar-se mais complexas, com o acréscimo de novas questões, como a confiança levantada por Guerra et al. (2002), em que salientavam naquela época haver uma tensão na relação de confiança destacando que a recolha e disponibilização de dados pode criar problemas de confiança em termos de privacidade, sendo esta, facilmente identificada como uma preocupação que impede os consumidores de usar a Internet para transações. Desta forma, há uma tensão na confiança entre a privacidade e identidade, a ausência de dados completos, como uma prestação de contas limitada, prejudica a confiança, mas a coleta de dados detalhados cria problemas de confiança em relação ao uso dos mesmos.

Estas questões estão intimamente ligadas as incertezas sobre a propriedade e controle dos dados e informações que as aplicações da IoT podem gerar. Atribuir propriedade dos dados recolhidos por meio da IoT em vários contextos que envolvem múltiplos atores, apresenta-se como um dos desafios iniciais para esse tipo de aplicação (ROCHELANDET; TAI, 2012).

Dutton (2014) comenta que em contextos tradicionais os direitos de autor dos dados e das informações geradas por máquinas são atribuídos ao operador do equipamento, contudo, tal entendimento pode não ser plenamente aplicado a redes de sensores de funcionamento autônomo. Da mesma forma, em alguns outros contextos, a propriedade é contestada, tal como com os dados de saúde, que podem pertencer simultaneamente a pacientes, hospitais, laboratórios e a controladores, em situações de pesquisa em que novos diagnósticos são criados, novos medicamentos testados e dados genômicos são registrados (DUTTON, 2005).

A Internet das Coisas tende a ampliar essa construção colaborativa, compartilhando aplicações e dados não apenas entre prestadores de serviços e consumidores, mas entre setores e cadeias produtivas inteiras, tornando ainda mais complexa a definição de propriedade (ASHRAF; HABAEBI, 2015).

A possibilidade de roubo ou outro acesso não autorizado aos dados ou sistemas desenvolvidos em torno da IoT significa que a segurança cibernética precisa ser vista como prioridade para a implementação de sistemas confiáveis. Estes sistemas têm de ser seguros a fim de estarem preparados para os mais variados cenários como

em caso de catástrofes naturais, de intrusão por quaisquer usuários não autorizados, para situações de violação de dados acidentais por parte de funcionários bem-intencionados com autorização a manipular dados (KIRK, 2012).

Evidencia-se que a implementação da arquitetura IoT ressalta uma série de desafios legais. Por tratar-se de um fenômeno global, existe a necessidade de estabelecer diretrizes gerais que possam ser adotadas pela legislação de todos os países a fim de proporcionar a padronização das ações, Weber e Weber (2010), destaca algumas das principais legislações que norteiam questões centrais a respeito da IoT.

O direito à privacidade, a protecção da privacidade individual livre de vigilância nacional e internacional, o rápido progresso alcançado no domínio das tecnologias da informação e, em particular, sobre a evolução, como as impressões digitais, monitoramento de rede, sistemas de bio-consciência, processamento eletrônico de dados, e criação extensas bases de dados, têm facilitado não só a coleta e armazenamento, mas também o processamento e interligação dos dados pessoais (ROCHELANDET; TAI, 2012; SAXBY, 2015).

Estes desenvolvimentos oferecem vantagens consideráveis em termos de eficiência e produtividade, mas também implica riscos potenciais. A tecnologia moderna oferece, em poucos segundos, o acesso a quantidades ilimitadas de dados pessoais e estabelece a possibilidade de criar perfis dos usuários, através da combinação de diferentes arquivos de dados, este é facilitado pela tecnologia de vigilância, podendo causar um aumento considerável no desrespeito a privacidade individual (GREER, 2006).

Neste sentido, diversos organismos internacionais preocupam-se com tais riscos definido em suas legislações o direito a privacidade, como o apresentado pelo art. 12 da Declaração Universal dos Direitos Humanos - DUDH, Art. 17 do Pacto Internacional sobre os Direitos Civis e Políticos - PIDCP, bem como o art. 8º da Convenção Europeia dos Direitos do Homem - CEDH (ALVES, 1999; PIOVESAN, 2006; COMPARATO, 2010). Além disso, no que concerne à Internet das Coisas como evolução da internet atual, iniciativas brasileiras recentes, como o marco civil da internet, buscam garantir a segurança do usuário, sua privacidade e a neutralidade da rede (URNAUER; MENNA BARRETO, 2015).

Na sociedade da informação a proteção de dados pessoais deve ser considerado uma questão-chave, em especial tendo em conta o direito de privacidade a proteção dos dados deve ser uma garantia essencial para o equilíbrio entre a vida privada, no que diz respeito as liberdades individuais e as exigências de segurança, e à necessidade de existir informações disponíveis (WEBER, 2010)**.**

Dentro dessa realidade Steffek e Nanz (2008) apresentam uma concepção de liberdade para a IoT, defendendo que os usuários devem ter total controle sobre etiquetas e sensores, podendo desativá-los sempre que desejarem, a fim de controlar a maneira como seus dados são coletados e utilizados. No que diz respeito a aplicação dos direitos humanos, parte-se do entendimento da proteção dos direitos individuais da pessoa humana, de sua individualidade perante a sociedade, resguardando-a das arbitrariedades do Estado e dos órgãos governamentais. Para tanto parte-se do principio que é da sociedade civil organizada que terá que surgir as iniciativas de regulamentação da privacidade na IoT (COMPARATO, 2010).

5. Considerações Finais

Por encontrar-se em estado inicial de desenvolvimento de aplicações, a IoT ainda não possui uma realidade de auto-regulamentação única, sendo regulada por variados padrões de negócios promovidos pela indústria que os conduzem a práticas justas de autorregulamentação da informação. Esta existência de autorregulação na IoT coincide com as experiências feitas no campo da governança da Internet em geral (WEBER; WEBER, 2010; BRODY; PURESWARAN, 2015), diante dessa realidade, sugere-se para pesquisas futuras no âmbito dos negócios a busca por elementos que constituam um código de privacidade universal capaz de contemplar negócios relacionadas a privacidade na IoT em setores diferentes.

Um acordo internacional vinculativo que abrange privacidade e proteção de dados ainda não existe. Mesmo que os instrumentos internacionais de direitos humanos tendam a vislumbrar na essência do uso da internet uma solução válida para a IoT, pelo menos até certo ponto, tais mecanismos não podem ser considerados suficientes, contudo, desde que não seja percebido como uma garantia universal, esta pode ser uma iniciativa pertinente para o fenômeno da Internet das Coisas (ATZORI; IERA ; MORABITO, 2010).

Portanto, é aceito que a co-regulação é necessária para garantir a implementação de princípios eficazes de privacidade no ambiente inteligente. Possíveis elementos de um sistema de autorregulação podem incluir códigos de conduta que contenham regras de boas práticas elaboradas em conformidade com a proteção da privacidade das pessoas, o estabelecimento de procedimentos de controlo interno, o ajuste de linhas diretas para lidar com as reclamações do público, e proteção de dados transparente (WEBER, 2010), neste sentido, sugere-se a realização de pesquisas voltadas para a unificação desses elementos já existentes para que possam alcançar uma regulamentação plena da privacidade dos usuários.

Tais iniciativas de padronização global da proteção da privacidade na IoT são de suma importância para a consolidação desse tipo de tecnologia, contudo, é importante destacar que a preocupação com a segurança e a

privacidade apresentadas pelas pessoas, não são identificas em localidades distintas do globo, o que torna a aplicação dos princípios gerais difíceis, principalmente quando trata-se de atividades comerciais entre diferentes países (WEBER, 2010; ROCHELANDET; TAI, 2012).

Dessa forma conclui-se que as soluções em regulamentação da privacidade existentes hoje para o mundo fisico não suportam as relações que a IoT potencialmente pode criar, assim como as políticas e regras de privacidade existentes nas relações virtuais ainda são incapazes de contemplar todas as potenciais explorações dos dados e informações dos usuários da IoT. Cabendo as instituições internacionais a tarefa de construir um quadro jurídico de base legal para regulamentar as práticas oriundas da IoT.

Referências

ALVES, José Augusto Lindgren. A declaração dos direitos humanos na pós-modernidade. **Os direitos humanos e o direito internacional. Rio de Janeiro: Renovar**, p. 139-166, 1999.

ASHRAF, Qazi Mamoon; HABAEBI, Mohamed Hadi. Autonomic schemes for threat mitigation in Internet of Things. **Journal of Network and Computer Applications**, v. 49, p. 112-127, 2015.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. **Computer networks**, v. 54, n. 15, p. 2787-2805, 2010.

BRODY, Paul; PURESWARAN, Veena. The next digital gold rush: how the internet of things will create liquid, transparent markets. **Strategy & Leadership**, v. 43, n. 1, p. 36-41, 2015.

CASTELLUCCIA, Claude et al. Privacy, accountability and Trust-Challenges and opportunities. **ENISA.[Online]. Available: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study/atdownload/fullReport**, 2011.

CHABRIDON, Sophie et al. A survey on addressing privacy together with quality of context for context management in the Internet of Things. **annals of telecommunications-annales des télécommunications**, v. 69, n. 1-2, p. 47-62, 2014.

COMPARATO, FABI0 KONDER. **A AFIRMAQAO HISTORICA DOS DIREITOS HUMANOS**. 2010. Tese de Doutorado. Universidade de Coimbra.

DANEZIS, George; GÜRSES, Seda. A critical review of 10 years of privacy technology. **Proceedings of Surveillance Cultures: A Global Surveillance Society**, 2010.

DUTTON, William H. The Internet and social transformation: reconfiguring access. Transforming enterprise: **The economic and social implications of information technology**, p. 375-397, 2005.

GAO, Lingling; BAI, Xuesong. A unified perspective on the factors influencing consumer acceptance of internet of things technology. **Asia Pacific Journal of Marketing and Logistics**, v. 26, n. 2, p. 211-231, 2014.

GREER, Steven. **The European Convention on Human Rights: achievements, problems and prospects**. Cambridge University Press, 2006.

GUBBI, Jayavardhana et al. Internet of Things (IoT): A vision, architectural elements, and future directions. **Future Generation Computer Systems**, v. 29, n. 7, p. 1645-1660, 2013.

GUERRA, G. A. et al. **Economics of trust: Trust and the information economy**. DSTI/ICCP/IE/REG (2002) 2, OECD, Paris and OII Research Report, 2003.

H. DUTTON, William. Putting things to work: social and policy challenges for the Internet of things. **info**, v. 16, n. 3, p. 1-21, 2014.

KRAUSE, Michael; HOCHSTATTER, Iris. Challenges in modelling and using quality of context (qoc). In: **Mobility aware technologies and applications**. Springer Berlin Heidelberg, 2005. p. 324-333.

LI, Shancang; DA XU, Li; ZHAO, Shanshan. The internet of things: a survey. **Information Systems Frontiers**, v. 17, n. 2, p. 243-259, 2014.

MARX, Gary T. Murky conceptual waters: The public and the private. **Ethics and Information technology**, v. 3, n. 3, p. 157-169, 2001.

MATOS, Alfredo Miguel Melo. Privacy in next generation networks. 2012.

MIORANDI, Daniele et al. Internet of things: Vision, applications and research challenges. **Ad Hoc Networks**, v. 10, n. 7, p. 1497-1516, 2012.

PANG, Zhibo et al. Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things. **Enterprise Information Systems**, v. 9, n. 1, p. 86-116, 2015.

PEOPLES, Cathryn et al. Performance evaluation of green data centre management supporting sustainable growth of the internet of things. **Simulation Modelling Practice and Theory**, v. 34, p. 221-242, 2013.

PIOVESAN, Flávia. Direitos humanos. **Curitiba: Juruá**, v. 1, p. 15-37, 2006.

ROCHELANDET, Fabrice; TAI, Silvio HT. Do privacy laws affect the location decisions of internet firms? Evidence for privacy havens. **European Journal of Law and Economics**, p. 1-30, 2012.

ROMAN, Rodrigo; NAJERA, Pablo; LOPEZ, Javier. Securing the internet of things. **Computer**, v. 44, n. 9, p. 51-58, 2011.

SAXBY, Steve. The 2014 CLSR-LSPI Lisbon seminar on 'the digital citizen'–Presented at the 9th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI) 15–17 October 2014, Vieira De Almeida & Associados, Lisbon, Portugal. **Computer Law & Security Review**, v. 31, n. 2, p. 163-180, 2015.

SOLOVE, Daniel J. A taxonomy of privacy. **University of Pennsylvania law review**, p. 477-564, 2006.

STEFFEK, Jens; NANZ, Patrizia. Emergent patterns of civil society participation in global and European governance. **Civil society participation in European and global governance: A cure for the democratic deficit**, p. 1-29, 2008.

URNAUER, Suellem Aparecida; MENNA BARRETO, Ricardo de Macedo. SEGURANÇA JURÍDICA NA CIBERCULTURA DE CONSUMO: REFLEXÕES À LUZ DA LEI Nº 12.965/2014 (MARCO CIVIL DA INTERNET). **Revista do Mestrado em Direito da Universidade Católica de Brasília: Escola de Direito**, v. 8, n. 2, p. 263-287, 2015.

VAIDYA, Jaideep. Privacy in the context of digital government. In: **Proceedings of the 13th Annual International Conference on Digital Government Research**. ACM, 2012. p. 302-303.

VALÉRY, N. Welcome to the Thingternet: Things, Rather than People, are About to Become the Biggest Users of the Internet. **The Economist**, v. 21, 2012.

VASSEUR, Jean-Philippe; DUNKELS, Adam. **Interconnecting smart objects with ip: The next internet**. Morgan Kaufmann, 2010.

WANG, Yang; KOBSA, Alfred. Privacy-enhancing technologies. **Handbook of Research on Social and Organisational Liabilities in Information Security**, p. 203-227, 2008.

WEBER, Rolf H. Internet of Things–New security and privacy challenges. **Computer Law & Security Review**, v. 26, n. 1, p. 23-30, 2010.

WEBER, Rolf H.; WEBER, Romana. **Internet of Things**. New York: Springer, 2010.