XIX encontro nacional de pesquisa em ciência da informação
ENANCIB
// SUJEITO INFORMACIONAL E AS PERSPECTIVAS ATUAIS EM CIÊNCIA DA INFORMAÇÃO. //
22-26 OUTUBRO 2018
LONDRINA/PR
Universidade Estadual de Londrina

XIX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2018

GT-8 – Informação e Tecnologia

INTERNET DAS COISAS E PRIVACIDADE: UMA REVISÃO SISTEMÁTICA DA LITERATURA

Jeferson Gonçalves de Oliveira (Universidade Fumec)

Paulo Augusto Isnard Santos (Universidade Fumec)

Cristiana Fernandes de Muylder (Universidade Fumec)

Rodrigo Moreno Marques (Universidade Fumec)

THE INTERNET OF THINGS AND PRIVACY: A SYSTEMATIC REVIEW OF LITERATURE

Modalidade da Apresentação: Comunicação Oral

Resumo: A Internet das Coisas (IoT) já transformou a sociedade, atingindo indústrias, cidades e lares e o valor econômico dessa transformação é estimado em trilhões de dólares. Juntamente com os potenciais benefícios dos dispositivos inteligentes interconectados, no ambiente IoT, aumentam o risco e o potencial de abuso ao incorporar detecção e inteligência em cada um dos dispositivos conectados. Assim, um dos principais problemas com o crescente número de dispositivos IoT é o aumento da complexidade para operá-los de forma segura, a fim de preservar a privacidade dos usuários. Dessa forma, este artigo buscou, por meio de uma revisão sistemática da literatura, responder a este problema com uma análise de artigos que abordem os métodos descritos para a garantia da privacidade dos usuários na IoT. Para isso, foram selecionados artigos a partir do ano de 2010, das bases *Web of Science*, *Scopus* e *Ebsco* e, como resultado, observa-se que a proteção dos dados pessoais, o comportamento do usuário, os aspectos legais e as formas de classificação da privacidade foram os temas mais citados. Percebe-se, assim, que são necessárias soluções que considerem esses temas de forma conjunta, não somente por meio de tecnologias, mas também de legislações e, principalmente, do empoderamento do usuário.

Palavras-Chave: Internet das coisas; Privacidade; Segurança da Informação.

Abstract: The Internet of Things (IoT) has already transformed society, reaching industries, cities and homes and the economic value of this transformation is estimated at trillions of dollars. Together with the potential benefits of interconnected smart devices in the IoT environment, they increase the risk and potential for abuse by incorporating detection and intelligence into each of the connected devices. Thus, a major problem with the growing number of IoT devices is the increased complexity to operate them securely in order to preserve the privacy of users. In this way, this article sought, through a systematic review of the literature, to answer this problem with an analysis of articles that address the methods described to guarantee the privacy of the users in IoT. For this purpose, articles were selected from 2010, from the Web of Science, Scopus and Ebsco databases, and as a result, it is observed that the protection of personal data, user behavior, legal aspects and forms of classification of privacy were the most frequently cited topics. It is thus perceived that solutions are needed that consider these themes together, not only through technologies, but also of legislation, and especially of user empowerment.

Keywords: Internet of things; Privacy; Information Security.

1 INTRODUÇÃO

O avanço tecnológico e a revolução informacional, ocorrida nos últimos anos, proporcionaram um ambiente ideal para a análise e cruzamento de dados. Porém, em uma direção contrária, a privacidade do indivíduo vem sendo continuamente violada, principalmente quando se trata da proteção dos seus dados pessoais em questões relacionadas ao consumo. Essa revolução informacional é marcada principalmente por três fenômenos: convergência da base tecnológica, dinâmica da indústria e o crescimento e expansão da *internet* (BARRETO JUNIOR, 2009).

Warren e Brandeis (1890) já entendiam, no século XIX, que a privacidade é o direito ou proteção que os indivíduos devem ter sobre a pessoa e a propriedade. Os autores mencionam que a vida privada e doméstica haviam sido invadidas pelas fotografias instantâneas e eventos jornalísticos, de modo que o que antes era sussurrado na intimidade de um *closet*, passaria a ser dito nas coberturas das casas. Nos dias atuais, a tecnologia, cada vez mais, impõe essas preocupações na sociedade moderna, de modo que esses riscos se ampliam e se tornam mais complexos.

Já o termo "*Internet of things*" (IoT), ou "Internet das Coisas", surgiu em 1999 e foi introduzido por Kevin Ashton, co-fundador e diretor executivo do *MIT Auto-ID Centre* (SUNDMAEKER; GUILLEMIN; FRIES, 2010). Segundo os autores, o termo Auto-ID refere-se a qualquer classe de tecnologias de identificação usadas na indústria com o intuito de

automatizar, reduzir erros e aumentar a eficiência. Em 2003, o principal foco Auto-ID foi a tecnologia de identificação por rádiofrequência (RFID).

Thierer (2015) define IoT como uma geração de objetos que permitem convergir atividades e exercem uma função de maneira sensitiva, automatizada e integrada, não limitando a *internet* somente ao uso de computadores, mas sim de qualquer tipo de objeto – carros, geladeiras, relógios, óculos dentre outros. Percebe-se que esse novo conceito resulta em registro e compartilhamento de dados comportamentais e de costumes, e, dessa forma, pode-se esperar que a privacidade na IoT pode abranger diferentes aspectos: técnicos, legais, comportamentais e de organização.

É nesta lacuna que surge a motivação deste estudo: quais são os métodos, apontados na literatura científica internacional, utilizados para garantir a privacidade na internet das coisas? O objetivo deste artigo é descrever esses métodos em pesquisas que abordaram uma conexão entre os dois temas: IoT e privacidade. Para isso, foi feita uma revisão sistemática da literatura em três bases de dados científicas - Scopus, Ebsco e *Web of Science* – em trabalhos publicados a partir de 2011 (ano que foi estabelecido um aumento substancial nas publicações científicas), nos idiomas português ou inglês. Especificamente, buscou-se: i) identificar estudos que façam uma abordagem conjunta dos dois temas; ii) identificar os focos temáticos dos estudos; iii) analisar métodos indicados para garantir a privacidade dos usuários na IoT.

Justifica-se o estudo realizado frente a necessidade acadêmica de descrever o estado da arte sobre o binômio privacidade e IoT e ainda propiciar novas discussões. O assunto é foco de investimento de trilhões de dólares e envolve transformação de indústrias, cidades e rotinas das pessoas em suas casas (WEBER, 2015). Além disso, a preservação da privacidade será um dos maiores desafios visto que bilhões de dispositivos serão implantados para coletar informações refinadas do ambiente para compartilhá-las com outros dispositivos (LOPEZ et al., 2017).

Na sequência, apresentam-se as seções de referencial teórico, metodologia, resultados e as considerações finais seguida das referências.

2 REFERENCIAL TEÓRICO

Nesta revisão da literatura buscou-se organizar os conceitos acerca dos temas IoT e privacidade.

2.1 Internet das coisas

A Internet das Coisas (IoT) pode ser considerada como a rede mundial de objetos interligados por meio de endereço exclusivo, com base em protocolos de comunicação padrão. Isso se dá por meio da coleta, do processamento e da análise de dados gerados pelos sensores da IoT, que se integrarão por meio dessa rede (Albertin & de Moura Albertin, 2017). O conceito de "coisa" tem evoluído junto à tecnologia, mas, o principal objetivo da IoT é obter informações úteis para sistemas computadorizados sem a intervenção humana (MISUGI; OBLADEN; FREITAS, 2016). Para isso, é necessária uma evolução na rede de objetos interconectados que passam a colher informações do ambiente (sensoriamento) e interagir com o mundo físico (atuação, comando e controle). Também são necessários novos padrões tecnológicos para a Internet que permitam serviços de transferência, análises e usos da informação (WEBER, 2015).

A IoT tem transformado indústrias, cidades e lares sendo possível estimar que esta transformação envolve trilhões de dólares relacionado à produtividade nos negócios (WEBER, 2015). Juntamente com os potenciais benefícios dos dispositivos conectados, aumentam os riscos e o potenciais de vulnerabilidade de dados pessoais. Um dos principais problemas com o crescente número de dispositivos IoT é a maior complexidade necessária para operá-los de forma segura e segura (MISUGI et al., 2016).

Esta complexidade cria novos desafios no âmbito da privacidade e usabilidade e este ambiente provoca tendências ou percepções de uso negativas. Busca-se determinar o melhor caminho para que os indivíduos gerenciem a privacidade de seus dados pessoais ao usar dispositivos. Para demonstrar a abrangência do tema, uma classificação das "coisas" em quatro áreas de aplicação e seus usuários finais é apresentada como padrão (FU et al., 2017):

- Casa: composto pela relação de saúde, entretenimento e eletrodomésticos.
- Transporte: representado pela logística.
- Comunidade: composta pelo meio ambiente de negócios.
- Nacional: sendo os usuários serviços públicos.

A IoT prevê a interconexão e a cooperação integrada de elementos inteligentes dentro de um ambiente de IoT, possibilitadas pela infraestrutura atual e futura da Internet. A IoT é, portanto, a evolução da internet, permitindo muitas novas aplicações que irão afetar o cotidiano das pessoas, gerar novos negócios e tornar, por exemplo, as cidades e os transportes mais inteligentes. Percebe-se, então, que o desenvolvimento da internet das coisas é crescente e

promissor e pode ser considerado indutor de inovações. Porém, ele traz ameaças à privacidade das pessoas, próximo tópico abordado neste referencial teórico.

2.2 Privacidade

Para o melhor entendimento de como a inovação tecnológica pode se tornar uma ameaça, é necessário compreender o conceito de privacidade que é muito amplo (SOLOVE, 2008). Segundo o autor, a privacidade abrange liberdade de pensamento, controle sobre o corpo, solidão, controle sobre informações pessoais, liberdade de vigilância, proteção da reputação dentre outros. Ressalta-se uma classificação de privacidade em seis definições diferentes: direito de ficar sozinho; acesso limitado ao "eu"; segredo; controle sobre as informações pessoais; personalidade e intimidade (SOLOVE, 2008).

Porém, Habermas (1987) mostra um modelo de sociedade moderna que permite conceitualizar a relação entre o privado e o público. Segundo o autor, a vida é composta pela esfera privada, representada pela família e intimidade, e a esfera pública que permite que pessoas privadas participem da cultura por meio de redes comunicativas e ajudem a formar uma opinião pública (HABERMAS, 1987, p.319). Essa distinção entre as esferas, pública e privada, é importante para distinguir entre o que deve ser mostrado e o que deve ser escondido (ARENDT, 1958, p.72).

Schoeman (1984) categoriza a privacidade como: reivindicação, direito; a medida do controle de um indivíduo sobre informações pessoais, intimidade e visibilidade; estado ou condição de acesso limitado a um indivíduo. Solove (2004) reforça a definição relacionada com o controle de informações pessoais com outras definições de privacidade: proteção do Big Brother; segredo; não invasão; controle sobre o uso da informação.

Segundo a teoria do controle da privacidade, a privacidade refere-se ao controle de informações sobre si mesmo e sobre o acesso a assuntos pessoais (TAVANI, 2008, p.142). Essa definição é corroborada por Westin (1967, p.7) que define privacidade como o direito de indivíduos, grupos ou instituições determinarem como, quando e em que medida as informações sobre eles serão comunicadas aos outros.

Silveira, Avelino e Souza (2016) concluem que o mercado de dados pessoais já é a principal fonte de receita em algumas partes da economia mundial. Os autores citam que o direito à privacidade será o principal limitador à expansão desse mercado, sendo que a transparência completa do cotidiano das pessoas tem sido buscada pelas forças do mercado.

Além disso, o interesse de vigilância por parte do Estado também busca restringir o direito à privacidade.

Dessa forma, o desenvolvimento da IoT deve seguir os princípios básicos de proteção da privacidade pessoal, por meio de leis, modelos de proteção à privacidade, regulamentações e tecnologias para garantir a inviolabilidade da privacidade pessoal, removendo, assim, obstáculos e barreiras para as suas aplicações (ZHANG; YE, 2010).

3 METODOLOGIA

A metodologia do presente estudo foi dividida em 2 etapas. A primeira consiste em aplicar técnicas de Cientometria e a segunda aborda a Revisão Sistemática da Literatura.

3.1 Cientometria

Segundo Freitas (2008), a bibliometria é um método usado para analisar e quantificar a bibliografia. Já a cientometria, segundo Purcell (2016), proporciona melhoria da organização científica e do planejamento racional da ciência. Essa é definida como o estudo da mensuração e quantificação do progresso científico, tendo potencial de aplicação, em instituições de pesquisas, do conhecimento com o objetivo de implementar diferentes formas de apoio ao desenvolvimento científico e tecnológico.

Dessa forma, a fim de utilizar outra metodologia e comprovar a validade do mapa empírico cognitivo de relacionamentos conceituais, foi utilizada a ferramenta *VOSviewer*, onde a associação se dá através de modelos *semi-logs* com análise de regressão e aparece na forma logarítmica (RODRIGUES; GODOY VIEIRA, 2016).

3.2 Revisão Sistemática da Literatura

O presente estudo baseia-se no modelo de revisão sistemática da literatura (RSL) proposto por Kitchenham (2004) que basicamente divide-se em três etapas: o planejamento da revisão, a condução da revisão e a análise dos resultados.

Na fase de planejamento foi estabelecido o protocolo para a execução da RSL que seguiu as seguintes etapas: a descrição dos objetivos, a elaboração da questão de pesquisa, descrição da estratégia de busca e a adoção dos critérios para inclusão/exclusão dos artigos.

O objetivo deste artigo é descrever estudos que abordaram relação entre os dois temas: IoT e privacidade. Para isso, foi feita uma revisão sistemática da literatura em três bases de

dados científicas - Scopus, Ebsco e *Web of Science* – em trabalhos publicados a partir de 2011 (ano que foi estabelecido um aumento substancial nas publicações científicas), nos idiomas português ou inglês com o intuito de responder à seguinte pergunta: quais são os as relações apresentadas entre privacidade na internet das coisas, apontados na literatura internacional?

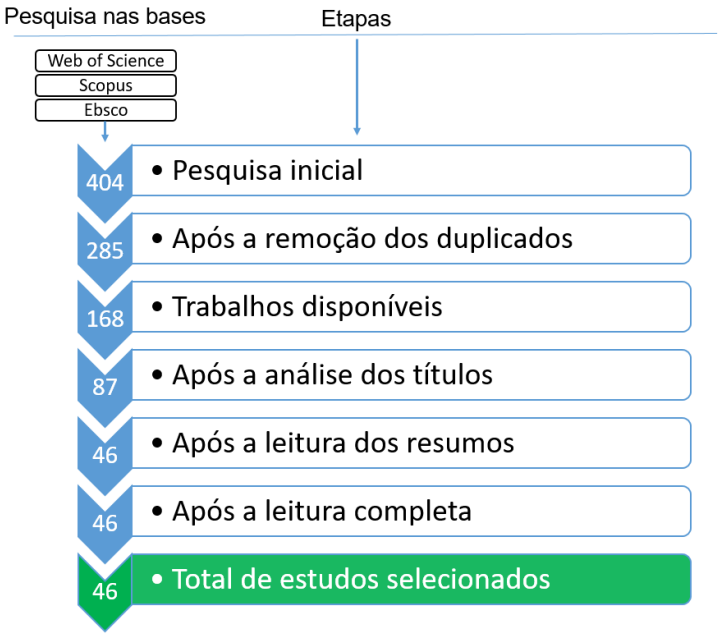
Com relação à estratégia de busca, o presente estudo baseia-se nos seguintes critérios: i) as bases de dados utilizadas no trabalho foram: *Web of Science*, Scopus e Ebsco; ii) elaboração da string de pesquisa: foi elaborada uma *string* que continha as palavras "privacidade" e "internet das coisas". Esses termos foram traduzidos para a língua inglesa e resultou no seguinte: *TITLE (("privacy" OR "privacidade") AND ("internet of things" OR "internet das coisas" OR "IOT")).*

Os critérios para inclusão e exclusão de trabalhos foram: i) para inclusão dos estudos: as publicações devem estar disponíveis na *Web*, especificamente nas bases selecionadas, abordando estudos sobre privacidade na internet das coisas e respondendo a qualquer uma das questões de pesquisa. Além disso, os artigos devem ter a sua data de publicação a partir de 2011. ii) para exclusão dos estudos: trabalhos duplicados, que não abordam o tema necessário, não respondam a nenhuma das questões de pesquisa ou possuem o ano de publicação anterior ao ano de 2011.

Após a recuperação dos estudos primários por meio da *string* de busca, os trabalhos foram organizados na ferramenta *ENDNOTE* X7 para facilitar a separação e o rastreamento de cada uma das fases e critérios de inclusão/exclusão.

Sendo assim, foram encontrados 404 estudos após a busca inicial nas bases. Após a remoção dos duplicados, obteve-se um total de 285 trabalhos. Destes, 117 não estavam disponíveis gratuitamente na *Web* e não foram recuperados. Dos 168 artigos restantes, 81 deles foram removidos após a análise dos títulos. Os 87 restantes tiveram a leitura dos seus resumos e essa fase resultou em 46 trabalhos conforme mostrado na Figura 1.

Figura 1 – Processo de recuperação e pré-seleção



Fonte: Elaborado pelos autores - 2018

Após as fases de recuperação e pré-seleção, os artigos foram analisados por meio de uma leitura completa do seu conteúdo. Assim, os 46 trabalhos selecionados na fase anterior foram selecionados.

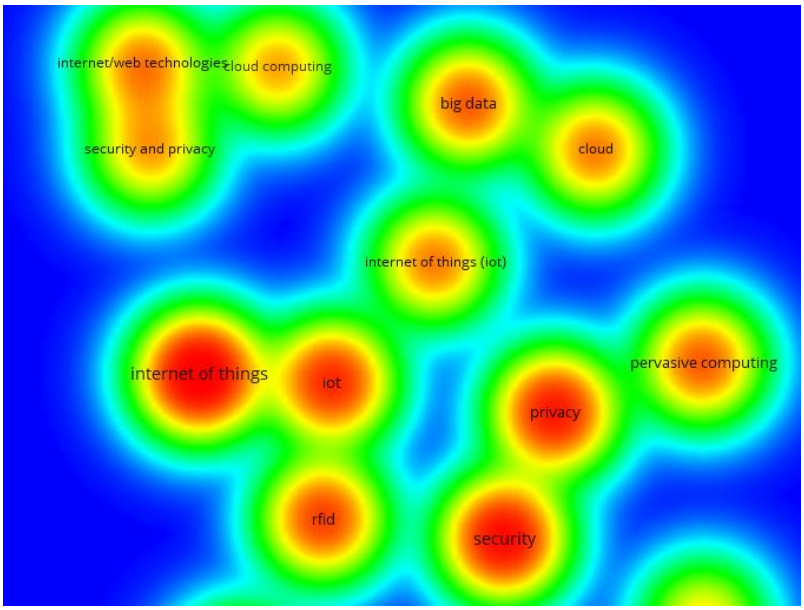
4 RESULTADOS E DISCUSSÕES

Os resultados foram apresentados em duas etapas, a cientometria e bibliometria.

4.1 Definição de clusters e mapa de relacionamento entre entidades conceituais

Para corroborar com os filtros da revisão sistemática da literatura, os 87 artigos selecionados para a fase de análise de títulos foram analisados. Os construtos privacidade e IoT que foram recuperados por meio da *string* de busca detalhada no capítulo de metodologia são exibidos em destaque no mapa de densidade. Dessa forma, é possível perceber graficamente a força interna dos vínculos de palavras-chave que compõem a rede temática (Figura 2).

Figura 2 – Mapa de densidade e relacionamento



Fonte: Elaborado pelos autores

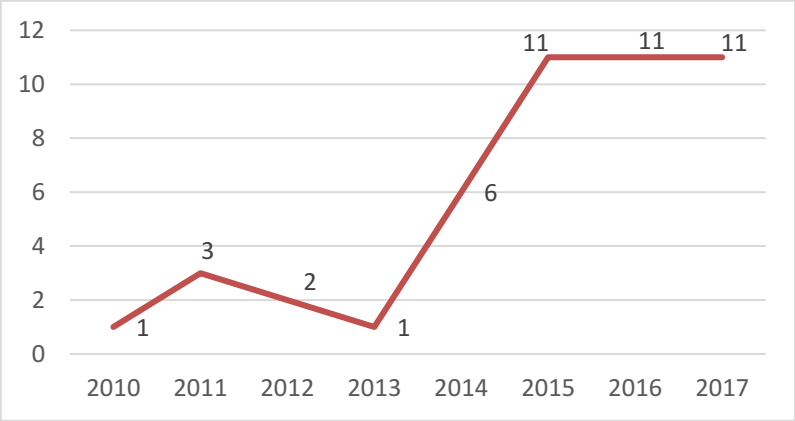
Segundo Choi (2005), a centralidade permite o uso de medidas para entender estruturas grupais, definindo a importância do tema no desenvolvimento e medindo o grau de interação com outras redes temáticas. Já a densidade de Callon descreve o grau de coesão interna, exprimindo a força interna dos vínculos (NALIMOV, 2016). Estas duas medidas permitem construir o Diagrama Estratégico da Rede Temática, um espaço bidimensional composto de quadrantes em que se distribuem os diversos temas (COBO; HERRERA, 2016).

Ao analisar a força de ligação entre os diversos componentes do cluster, que surge a partir das pesquisas bibliográficas realizadas, nota-se claramente, na Figura 2, o destaque dos termos “Segurança” e “Privacidade”. Este detalhe corrobora com a intenção inicial do artigo de verificar a convergência destes termos com IoT, entretanto, não é possível identificar, somente por meio do mapa de relacionamento, nos construtos “Segurança” e “Privacidade”, os aspectos meramente técnicos e distingui-los dos aspectos sociais. Dessa forma, o presente estudo utilizou a leitura individual das publicações selecionadas no protocolo de revisão sistemática da literatura.

4.2 Revisão sistemática da literatura

Em relação ao ano de publicação, a revisão sistemática da literatura mostra uma concentração de estudos após o ano de 2014, conforme a Figura 3:

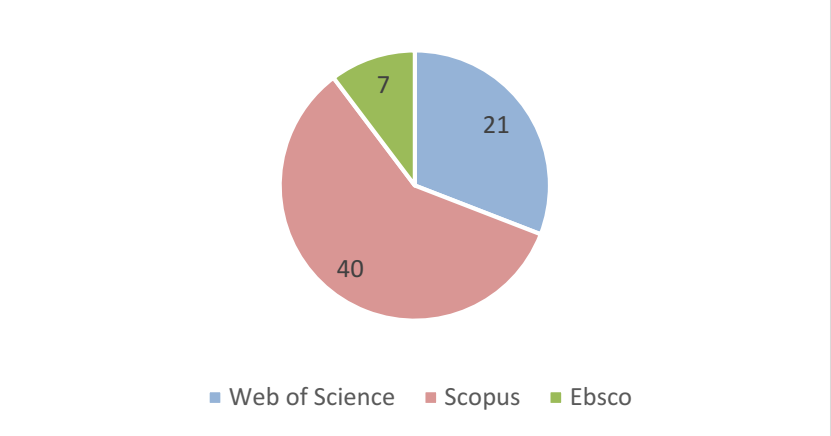
Figura 3 – Distribuição dos 46 estudos por ano de publicação



Fonte: Dados da pesquisa

A distribuição dos 46 artigos selecionados por bases pesquisadas mostra que a grande maioria, 40 deles, foram encontrados na base Scopus. A base *Web of Science* totalizou 21 artigos e a base Ebsco somente 7 trabalhos. A soma total supera a quantidade de 46 trabalhos porque muitos deles foram encontrados em mais de uma base e foram removidos posteriormente (Figura 4).

Figura 4 – Distribuição dos 46 estudos por base de pesquisa



Fonte: Dados da pesquisa

Em relação ao foco do estudo, os 46 artigos são descritos e categorizados abaixo, no Quadro 1, em ordem cronológica:

QUADRO 1: Os principais focos temáticos dos 46 estudos selecionados

Nº	REFERÊNCIA	FOCO TEMÁTICO DO ESTUDO
1	Weber (2010)	Aspectos legais
2	Hu, Zhang e Wen (2011)	Proteção dos dados dos usuários
3	Liang e Peiji (2011)	Proteção dos dados dos usuários
4	Tao e Peiran (2011)	Classificação de privacidade
5	Elkhodr, Shahrestani e Cheung (2012)	Proteção dos dados dos usuários

6	Ukil et al. (2012)	Proteção dos dados dos usuários
7	Alcaide et al. (2013)	Proteção dos dados dos usuários
8	Henze et al. (2013)	Proteção dos dados dos usuários
9	Lu et al. (2014)	Classificação de privacidade
10	Sun et al. (2014)	Proteção dos dados dos usuários
11	Ukil, Bandyopadhyay e Pal (2014)	Gerenciamento da privacidade
12	Wong e Kim (2014)	Proteção dos dados dos usuários
13	Ziegeldorf, Morchon e Wehrle (2014)	Desafios da privacidade
14	Funke et al. (2015)	Políticas de privacidade
15	Lu et al. (2015)	Classificação de privacidade
16	Samani, Ghenniwa e Wahaishi (2015)	Framework de privacidade
17	Sanchez-Alcon, Lopez-Santidrian e Martinez (2015)	Proteção dos dados dos usuários
18	Schurgot, Shinberg e Greenwald (2015)	Proteção dos dados dos usuários
19	Smith (2015)	Prós e contras da privacidade
20	Ukil, Bandyopadhyay e Pal (2015)	Proteção dos dados dos usuários
21	Vasilomanolakis et al. (2015)	Análise de arquitetura de IoT
22	Weber (2015)	Aspectos legais
23	Weinberg (2015)	Proteção dos dados dos usuários
24	Zhou e Piramuthu (2015)	Personalização da privacidade
25	Bailey (2016)	Comportamento do usuário
26	Bertino (2016)	Proteção dos dados dos usuários
27	Caron et al. (2016)	Aspectos legais
28	Harris, Sundaram e Kravets (2016)	Proteção dos dados dos usuários
29	Hsu e Lin (2016)	Comportamento do usuário
30	Malina et al. (2016)	Proteção dos dados dos usuários
31	Mehotra et al. (2016)	Proteção dos dados dos usuários
32	Misugi, de Almeida Freitas e Carlos Efing (2016)	Dimensões da privacidade
33	Strazdins e Wang (2016)	Desafios da privacidade
34	Suryani, Sulistyo e Widyawan (2016)	Classificação de privacidade
35	Williams, Nurse e Creese (2016)	Comportamento do usuário
36	Chamberlain et al. (2017)	Comportamento dos usuários, aspectos legais e proteção de dados pessoais
37	Conoscenti, Vetro e De Martin (2017)	Proteção dos dados dos usuários
38	Concoran (2017)	Framework de privacidade
39	Jayaraman et al. (2017)	Proteção dos dados dos usuários
40	Lee e Kodsa (2017)	Comportamento do usuário
41	Lopez et al. (2017)	Desafios da privacidade
42	Madaan, Ahad e Sastry (2017)	Proteção dos dados dos usuários
43	O'Connor et al. (2017)	Proteção dos dados dos usuários
44	Segu (2017)	Proteção dos dados dos usuários
45	Tran (2017)	Aspectos legais
46	Zhou et al. (2017)	Proteção dos dados dos usuários

Fonte: Dados da Pesquisa

No Quadro 1 é possível observar que 24 estudos, de um total de 46 selecionados, possuem um enfoque na questão de proteção dos dados dos usuários. Nestes, a grande maioria trata de questões técnicas como criptografia de dados, algoritmos, protocolos de autenticação e técnicas de pseudônimos como formas de manter essa proteção (Quadro 2).

QUADRO 2: Os métodos citados para a proteção dos dados dos usuários na IoT

Nº	REFERÊNCIA	MÉTODO ABORDADO PARA PROTEÇÃO DOS DADOS
1	Hu, Zhang e Wen (2011)	Autenticação com o uso de identidades virtuais
2	Liang e Peiji (2011)	Algoritmo de proteção dos dados
3	Elkhodr, Shahrestani e Cheung (2012)	Não cita métodos. Alerta sobre o perigo do rastreamento que já existe na computação móvel e pode ser herdada pela IoT
4	Ukil et al. (2012)	Mascaramento de dados por método similar à criptografia
5	Alcaide et al. (2013)	Protocolo de autenticação anônimo e descentralizado
6	Henze et al. (2013)	Cita o UPECSI, um sistema de controle de privacidade baseados em serviços na nuvem
7	Sun et al. (2014)	Algoritmo de homomorfismo
8	Wong e Kim (2014)	Protocolo de coleta de dados de autoconsciência
9	Sanchez-Alcon, Lopez-Santidrian e Martinez (2015)	Não cita um método específico. Mostra que a combinação das áreas empresarial, jurídica e tecnológica podem oferecer as melhores soluções
10	Schurgot, Shinberg e Greenwald (2015)	Criptografia dos dados
11	Ukil, Bandyopadhyay e Pal (2015)	Propõe uma solução DPA (*Dynamic Privacy Analizer*)
12	Weinberg (2015)	Também não cita um método específico. Foca no dilema entre conveniência e privacidade
13	Bertino (2016)	Criptografia dos dados e segurança de aplicativos
14	Harris, Sundaram e Kravets (2016)	Apresenta o Lamina, um sistema para prover privacidade baseado em criptografia e mecanismos de mudanças de endereços MAC
15	Malina et al. (2016)	Criptografia dos dados
16	Mehotra et al. (2016)	Criptografia dos dados
17	Chamberlain et al. (2017)	Não cita um método específico. Fala sobre proteção dos dados, comportamento dos usuários e aspectos legais
18	Conoscenti, Vetro e De Martin (2017)	Propõe um sistema distribuído ponto-a-ponto
19	Jayaraman et al. (2017)	Criptografia dos dados
21	Madaan, Ahad e Sastry (2017)	Não apresenta método. Os autores discutem a ameaça à privacidade por meio do *link* de informações
22	O'Connor et al. (2017)	Consentimento dos usuários (*eConsent*)
23	Segu (2017)	Consentimento dos usuários
24	Zhou et al. (2017)	Criptografia dos dados

Fonte: Dados da Pesquisa

Porém, 5 dos trabalhos selecionados focam na questão legal sobre a privacidade na IoT (WEBER, 2010; WEBER, 2015; CARON et al., 2016; CHAMBERLAIN et al., 2017; TRAN, 2017). Estes pesquisadores citam a importância de uma legislação específica para garantir a privacidade das pessoas e afirmam que questões técnicas não são suficientes para tal se abordadas de forma isolada. As abordagens jurídicas precisam considerar diferenças na legislação sobre questões de comunicação e controle relacionadas às preocupações da IoT.

Em relação ao comportamento do usuário, o estudo encontrou 5 artigos (BAILEY, 2016; HSU; LIN, 2016; WILLIAMS, NURSE; CREESE, 2016; CHAMBERLAIN et al., 2017; LEE; KODSA, 2017). Estes artigos demonstram que o comportamento e atitude do usuário em um ambiente

de IoT tem reflexos diretos no aspecto privacidade e pesquisas de opinião mostram que os indivíduos afirmam valorizar a privacidade. Sendo assim, compreender o que as pessoas pensam sobre a tecnologia, sua vontade de adotá-la e seus desafios em mantê-la precisam ser uma parte crítica da pesquisa e da política da IoT.

Outros 4 estudos focam na questão da classificação da privacidade (TAO; PEIRAN, 2011; LU et al., 2014; LU et al., 2015; SURYANI, SALISTYO; WIDYAWAN, 2016). Esses estudos citam a necessidade de classificar a privacidade em níveis e outros estudos usam algoritmos para classificação de objetos confiáveis. A classificação é uma forma de organização necessária para inclusive amparar aspectos legais da privacidade da IoT. Também sugerem que essa classificação possa ser de responsabilidade compartilhada com os usuários, que indicariam os dados a serem considerados sensíveis.

Assim, 38 dos 46 artigos abordaram 4 temas principais (Quadro 01): proteção de dados dos usuários, aspectos legais, comportamento do usuário e classificação da privacidade. Isso representa aproximadamente 83% do total de trabalhos selecionados e mostram que a maioria dos estudos selecionados consideram estas dimensões de atuação em relação à privacidade na IoT.

5 DISCUSSÕES

A privacidade abrange conceitos como: liberdade de pensamento, controle sobre o corpo, solidão, controle sobre as informações pessoais, liberdade de vigilância e proteção da reputação. O autor preconiza uma classificação com as seguintes definições: direito de ficar sozinho; acesso limitado ao “eu”; segredo; controle sobre as informações pessoais; personalidade e intimidade (SOLOVE, 2008).

Após a revisão da literatura, nota-se que os principais métodos abordados para a proteção dos dados dos usuários foram: criptografia de dados, algoritmos, protocolos de autenticação e técnicas de pseudônimos. Levando-se em conta que apenas 02 estudos citaram formas de rever o consentimento do usuário, fica a preocupação sobre o entendimento de que a segurança na transmissão dos dados pessoais tem importância maior sobre o direito de um indivíduo de fornecer ou não o seu consentimento sobre os mesmos.

Além disso, somente 05 estudos (WEBER, 2010; WEBER, 2015; CARON et al., 2016; CHAMBERLAIN et al., 2017; TRAN, 2017) abordaram as questões legais sobre a privacidade na IoT período analisado. Percebe-se, novamente, que as discussões acadêmicas estão focadas nas

tecnologias de proteção dos dados, e questões como a legalidade e o consentimento do usuário foram pouco exploradas.

O desenvolvimento da IoT deve seguir os princípios básicos de proteção da privacidade pessoal não por meio somente de tecnologias, mas também de: leis, modelos de proteção à privacidade e regulamentações para garantir a inviolabilidade dos dados pessoais, removendo, assim, obstáculos e barreiras para as suas aplicações (ZHANG; YE, 2010).

Esses princípios são reforçados pela teoria do controle da privacidade, que se refere ao controle de informações sobre si mesmo e sobre o acesso a assuntos pessoais (TAVANI, 2008, p.142). Essa premissa é apontada por Westin (1967, p.7) que define privacidade como o direito de indivíduos, grupos ou instituições determinarem como, quando e em que medida as informações sobre eles serão comunicadas publicamente.

Portanto, o empoderamento do indivíduo em relação à sua privacidade ainda é pouco discutido no meio acadêmico, embora seja muito necessário. Contudo, também é necessária uma legislação que ampare todo este processo e que garanta a validade e a obrigatoriedade deste consentimento, não bastando somente os cuidados tecnológicos na transmissão e no armazenamento dos dados.

6 CONSIDERAÇÕES FINAIS

O avanço tecnológico e a revolução informacional possibilitam um ambiente favorável para o cruzamento de dados e análises estatísticas. Porém, a privacidade do indivíduo vem sendo constantemente violada, principalmente em se tratando dos seus dados pessoais. A *Internet* das Coisas acompanha essa evolução tecnológica mas possibilita o compartilhamento de dados comportamentais e de costumes, aumentando, assim, os riscos de perda de privacidade.

Os novos produtos e serviços da IoT nos tornarão mais eficientes, com maior capacidade de atuação e compreensão e haverá novos aplicativos que nos permitirão maior interatividade. No entanto, é necessário aprender a conviver com uma grande quantidade de elementos que compõe a IoT e que reunirão informações sobre nossas atividades ameaçando a nossa privacidade. A desconfiança, e por consequência o afastamento, poderia ser uma barreira para o desenvolvimento completo desses novos produtos e serviços.

O presente estudo apresenta revisão sistemática da literatura baseada no protocolo proposto por Kitchenham (2004) e identifica os estudos publicados em relação aos temas IoT e

privacidade, permitindo uma análise do cenário abordado no meio acadêmico. Foram selecionados artigos a partir do ano de 2010, das bases *Web of Science,* Scopus e Ebsco. Dos 286 estudos encontrados (não duplicados), apenas 46 foram selecionados devido à falta de aderência com a temática.

Os resultados indicaram que 83% desses artigos tratam dos seguintes temas: proteção de dados pessoais (24 artigos), aspectos legais da privacidade na IoT (5 artigos), comportamento do usuário (5 artigos) e classificação da privacidade (4 artigos). Percebe-se, nessa revisão, que esses temas estão interconectados e, para garantir a privacidade na IoT, são necessárias soluções que considerem esses aspectos de forma conjunta, não somente por meio de tecnologias, mas também por meio de legislações e do empoderamento do usuário.

Embora a metodologia do artigo proposto não busque esgotar o assunto e, considerando que ocorre limitação a subjetividade, sugere-se novos estudos que propiciem discussão acerca da relação entre os quatro temas: proteção de dados pessoais, aspectos legais da privacidade na IoT, comportamento do usuário e classificação da privacidade.

REFERÊNCIAS

ALBERTIN, Alberto Luiz; DE MOURA ALBERTIN, Rosa Maria. A internet das coisas irá muito além as coisas. **GV-executivo**, v. 16, n. 2, p. 12-17, 2017.

ALCAIDE, Almudena et al. Anonymous authentication for privacy-preserving IoT target-driven applications. **Computers & Security**, v. 37, p. 111-123, 2013.

ARENDT, Hannah. **The Human Condition**. University of Chicago Press, Chicago, 1993.

BAILEY, Melissa W. Seduction by Technology: Why Consumers Opt out of Privacy by Buying into the Internet of Things. **Tex. L. Rev.**, v. 94, p. 1023, 2015.

BARRETO JUNIOR, Irineu Francisco. Abordagens recentes da pesquisa jurídica na Sociedade da Informação. In: PAESANI, Liliana Minardi. (Coord.). **O direito na sociedade de informação II**. São Paulo: Atlas, 2009.

BERTINO, Elisa. Data privacy for IoT systems: concepts, approaches, and research directions. In: **Big Data (Big Data), 2016 IEEE International Conference on**. IEEE, 2016. p. 3645-3647.

CARON, Xavier et al. The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. **Computer Law & Security Review**, v. 32, n. 1, p. 4-15, 2016.

CHAMBERLAIN, Alan et al. Special theme on privacy and the Internet of things. 2017.

CHOI, Hyun. **TOT: the association strength heuristic**. 2005. Tese de Doutorado. Texas A&M

University.

COBO, Manolo J. et al. SciMAT: A new science mapping analysis software tool. **Journal of the Association for Information Science and Technology**, v. 63, n. 8, p. 1609-1630, 2012.

CONOSCENTI, Marco; VETRÒ, Antonio; DE MARTIN, Juan Carlos. Peer to Peer for Privacy and Decentralization in the Internet of Things. In: **Proceedings of the 39th International Conference on Software Engineering Companion**. IEEE Press, 2017. p. 288-290.

CORCORAN, Peter M. A privacy framework for the Internet of Things. In: **Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on**. IEEE, 2016. p. 13-18.

DA SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, v. 12, n. 1, 2017.

ELKHODR, Mahmoud; SHAHRESTANI, Seyed; CHEUNG, Hon. A review of mobile location privacy in the internet of things. In: **ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on**. IEEE, 2012. p. 266-272.

FREITAS, H. M. R. Análise de dados qualitativos: aplicação e tendências mundiais em sistemas de informação. **Revista de Administração-RAUSP**, v. 35, n. 4, p. 84-102, 2000.

FU, Kevin et al. **Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things**. Technical Report. Computing Community Consortium, 2017.

FUNKE, Sebastian et al. End-2-End privacy architecture for IoT. In: **Communications and Network Security (CNS), 2015 IEEE Conference on**. IEEE, 2015. p. 705-706.

HABERMAS, Jurgen; HABERMAS, Jürgen. **The theory of communicative action**. Beacon press, 1985.

HARRIS, Albert F.; SUNDARAM, Hari; KRAVETS, Robin. Security and Privacy in Public IoT Spaces. In: **Computer Communication and Networks (ICCCN), 2016 25th International Conference on**. IEEE, 2016. p. 1-8.

HENZE, Martin et al. User-driven privacy enforcement for cloud-based services in the internet of things. In: **Future Internet of Things and Cloud (FiCloud), 2014 International Conference on**. IEEE, 2014. p. 191-196.

HSU, Chin-Lung; LIN, Judy Chuan-Chuan. An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. **Computers in Human Behavior**, v. 62, p. 516-527, 2016.

HU, Chunye; ZHANG, Jie; WEN, Qiaoyan. An identity-based personal location system with protected privacy in IoT. In: **Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on**. IEEE, 2011. p. 192-195.

JAYARAMAN, Prem Prakash et al. Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. **Future Generation Computer Systems**, 2017.

LEE, Hosub; KOBSA, Alfred. Understanding user privacy in Internet of Things environments. In: **Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on**. IEEE, 2016. p. 407-412.

LIANG, Wu; PEIJI, Shao. Research on the protection algorithm and model of personal privacy information in internet of thing. In: **E-Business and E-Government (ICEE), 2011 International Conference on**. IEEE, 2011. p. 1-4.

LOPEZ, Javier et al. Evolving privacy: From sensors to the Internet of Things. **Future Generation Computer Systems**, v. 75, p. 46-57, 2017.

LU, Xiaofeng et al. Privacy information security classification study in internet of things. In: **Identification, Information and Knowledge in the Internet of Things (IIKI), 2014 International Conference on**. IEEE, 2014. p. 162-165.

LU, Xiaofeng et al. Privacy information security classification for internet of things based on internet data. **International Journal of Distributed Sensor Networks**, v. 11, n. 8, p. 932941, 2015.

MADAAN, Nishtha; AHAD, Mohd Abdul; SASTRY, Sunil M. Data integration in IoT ecosystem: Information linkage as a privacy threat. **Computer Law & Security Review**, 2017.

MALINA, Lukas et al. On perspective of security and privacy-preserving solutions in the internet of things. **Computer Networks**, v. 102, p. 83-95, 2016.

MEHROTRA, Sharad et al. TIPPERS: A privacy cognizant IoT environment. In: **Pervasive Computing and Communication Workshops (PerCom Workshops), 2016 IEEE International Conference on**. IEEE, 2016. p. 1-6.

MISUGI, Guilherme; DE ALMENDRA FREITAS, Cinthia Obladen; EFING, Antonio Carlos. Releitura da Privacidade Diante das Novas Tecnologias: Realidade Aumentada, Reconhecimento Facial e Internet das Coisas. **Revista Jurídica Cesumar-Mestrado**, v. 16, n. 2, p. 427-453, 2016.

Nalimov, A. (2016). SCIENTOMETRICS: AN INNOVATIVE TOOL. In SCIENTOMETRICS (pp. 124–142).

O'CONNOR, Yvonne et al. Privacy by Design: Informed Consent and Internet of Things for Smart Health. **Procedia Computer Science**, v. 113, p. 653-658, 2017.

Purcell, C. (2016). Principles of Data Reduction. Journal of University of Sydney.

RODRIGUES, Charles; VIERA, Angel Freddy Godoy. Estudos bibliométricos sobre a produção

científica da temática Tecnologias de Informação e Comunicação em bibliotecas. **InCID: Revista de Ciência da Informação e Documentação**, v. 7, n. 1, p. 167-180, 2016.

SAMANI, Afshan; GHENNIWA, Hamada H.; WAHAISHI, Abdulmutalib. Privacy in Internet of Things: A model and protection framework. **Procedia Computer Science**, v. 52, p. 606-613, 2015.

SANCHEZ-ALCON, Jose-Antonio; LOPEZ-SANTIDRIAN, Lourdes; MARTINEZ, Jose-Fernan. Solution to ensure privacy in the internet of things. **PROFESIONAL DE LA INFORMACION**, v. 24, n. 1, p. 62-70, 2015.

SCHOEMAN, Ferdinand. Privacy: philosophical dimensions. **American Philosophical Quarterly**, v. 21, n. 3, p. 199-213, 1984.

SENGUL, Cigdem. Privacy, consent and authorization in IoT. In: **Innovations in Clouds, Internet and Networks (ICIN), 2017 20th Conference on**. IEEE, 2017. p. 319-321.

SCHURGOT, Mary R.; SHINBERG, David A.; GREENWALD, Lloyd G. Experiments with security and privacy in IoT networks. In: **World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a**. IEEE, 2015. p. 1-6.

SMITH, M.S. Protecting privacy in an IoT-connected world. **Information Management**, v. 49, n. 6, p. 36, 2015.

SOLOVE, Daniel J. **The digital person: Technology and privacy in the information age**. NyU Press, 2004.

SOLOVE, Daniel J. Understanding privacy. 2008.

STRAZDINS, Girts; WANG, Hao. Open security and privacy challenges for the internet of things. In: **Information, Communications and Signal Processing (ICICS), 2015 10th International Conference on**. IEEE, 2015. p. 1-4.

SUN, Guozi et al. A privacy protection policy combined with privacy homomorphism in the internet of things. In: **Computer Communication and Networks (ICCCN), 2014 23rd International Conference on**. IEEE, 2014. p. 1-6.

SUNDMAEKER, Harald et al. Vision and challenges for realising the Internet of Things. **Cluster of European Research Projects on the Internet of Things, European Commision**, v. 3, n. 3, p. 34-36, 2010.

SURYANI, Vera; SULISTYO, Selo; WIDYAWAN, Widyawan. Trust-Based Privacy for Internet of Things. **International Journal of Electrical and Computer Engineering**, v. 6, n. 5, p. 2396, 2016.

TAO, Hu; PEIRAN, Wang. Preference-based privacy protection mechanism for the internet of things. In: **Information Science and Engineering (ISISE), 2010 International Symposium on**.

IEEE, 2010. p. 531-534.

THIERER, Adam D. The internet of things and wearable technology: addressing privacy and security concerns without derailing innovation. **Richmond Journal of Law & Technolog y,** v. 21, n. 2, 2015.

TRAN, Alexander H. The Internet of Things and Potential Remedies in Privacy Tort Law. **Colum. JL & Soc. Probs.**, v. 50, p. 263, 2016.

UKIL, Arijit et al. Negotiation-based privacy preservation scheme in internet of things platform. In: **Proceedings of the First International Conference on Security of Internet of Things**. ACM, 2012. p. 75-84.

UKIL, Arijit; BANDYOPADHYAY, Soma; PAL, Arpan. Iot-privacy: To be private or not to be private. In: **Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on**. IEEE, 2014. p. 123-124.

UKIL, Arijit; BANDYOPADHYAY, Soma; PAL, Arpan. Privacy for IoT: Involuntary privacy enablement for smart energy systems. In: **Communications (ICC), 2015 IEEE International Conference on**. IEEE, 2015. p. 536-541.

VASILOMANOLAKIS, Emmanouil et al. On the Security and Privacy of Internet of Things Architectures and Systems. In: **Secure Internet of Things (SIoT), 2015 International Workshop on**. IEEE, 2015. p. 49-57.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review, v. 4, n. 5, 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm> Acesso em: 30 jul. 2015.

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. Internet of things: Privacy issues revisited. **Computer Law & Security Review**, v. 31, n. 5, p. 618-627, 2015.

WEINBERG, Bruce D. et al. Internet of Things: Convenience vs. privacy and secrecy. **Business Horizons**, v. 58, n. 6, p. 615-624, 2015.

WESTIN, Alan F. Privacy and freedom, atheneum. **New York**, v. 7, 1967.

WILLIAMS, Meredydd; NURSE, Jason RC; CREESE, Sadie. The perfect storm: The privacy paradox and the Internet-of-Things. In: **Availability, Reliability and Security (ARES), 2016 11th International Conference on**. IEEE, 2016. p. 644-652.

WONG, Kok-Seng; KIM, Myung Ho. Towards self-awareness privacy protection for Internet of things data collection. **Journal of Applied Mathematics**, v. 2014, 2014.

ZHANG, Jing; YE, Liuqi. The Internet of Things and Personal privacy Protection. In: **ICLEM 2010: Logistics For Sustained Economic Development: Infrastructure, Information, Integration**. 2010. p. 2892-2898.

ZHOU, Jun et al. Security and privacy for cloud-based IoT: challenges. **IEEE Communications Magazine**, v. 55, n. 1, p. 26-33, 2017.

ZHOU, Wei; PIRAMUTHU, Selwyn. Information relevance model of customized privacy for IoT. **Journal of Business Ethics**, v. 131, n. 1, p. 19-30, 2015.

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.