UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM INTERNET DAS COISAS

SARAH GOMES SAKAMOTO

SEGURANÇA, PRIVACIDADE E BLOCKCHAIN NO CONTEXTO DE INTERNET DAS COISAS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2020

SARAH GOMES SAKAMOTO

SEGURANÇA, PRIVACIDADE E BLOCKCHAIN NO CONTEXTO DE INTERNET DAS COISAS

Monografia de Especialização, apresentada ao Curso de Especialização em Internet das Coisas, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Jamil de Araujo Farhat

CURITIBA
2020

TERMO DE APROVAÇÃO

SEGURANÇA, PRIVACIDADE E BLOCKCHAIN NO CONTEXTO DE INTERNET DAS COISAS

por

SARAH GOMES SAKAMOTO

Esta monografia foi apresentada em 20 de Fevereiro de 2020 como requisito parcial para a obtenção do título de Especialista em Internet das Coisas. A candidata foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Jamil de Araujo Farhat
Orientador

_____
Prof. M. Sc. Danillo Leal Belmonte
Membro titular

_____
Prof. M. Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho a todos que participaram da minha vida, contribuíram para minha história e me apoiaram para que este momento acontecesse.

Serendipity.

AGRADECIMENTOS

Agradeço, primeiramente, pela oportunidade de continuar aprimorando meus conhecimentos em áreas de interesse profissional e de tamanha relevância. O destino é realmente intrigante e, ao repensar meus passos anteriores de pesquisa, mesmo que desviasse por outros caminhos e temas, acabo convergindo para pontos de intersecção, ainda que em diferentes contextos. Iniciação científica com RSSF, a inserção de fatores humanos com acessibilidade e engenharia de requisitos na graduação, pesquisa em *smart home*, IHC e dispositivos móveis durante o mestrado. Por fim, esperando voltar às minhas origens de redes, acabei permeando o domínio de segurança e trazendo a privacidade, alcançando ainda o universo jurídico.

Agradeço ao meu orientador, pela paciência e revisão deste trabalho, além de sua contribuição inestimada ao estruturar juntamente comigo este tema. Também agradeço ao professor Omero, pela possibilidade de concluir este trabalho com minha turma. Agradeço ainda aos meus pais, pelo auxílio financeiro e suporte em alcançar meus objetos; ao Alessandro, meu incrível companheiro de vida, maior suporte em minha jornada acadêmica e vida pessoal, a quem nunca terei condições suficientes de agradecer por toda sua contribuição em todas as minhas conquistas; ao Samoel, meu companheiro na breve jornada da vida, pelo suporte necessário para minha evolução pessoal e por, indiretamente, ser fundamental na minha compreensão de conceitos relacionados à privacidade.

Aos meus amigos docentes, colegas de profissão, da UTFPR Ponta Grossa, por fomentarem meu interesse de estudo, mesmo que ainda não em um doutorado; aos amigos que fiz como servidora na UFRGS, por compartilharem conhecimentos de redes e infraestrutura, além do curso de Blockchain; aos amigos e colegas de trabalho na Defensoria Pública, pelas oportunidades de atuação na área meio em uma instituição de tanta relevância na área fim; ao Sérgio, meu professor da Academia Cisco, pela indicação e por tratar do tema IoT; a todos os professores desta especialização, pela excelência no ensino, abordagens práticas e didáticas, além do tratamento igualitário em cada uma das disciplinas, mesmo sendo a única representante feminina na turma; e aos meus amigos da turma de CEIOT 2018, com quem compartilhei tantas sextas e sábados, meus profundos agradecimentos.

Deixo aqui um resultado sucinto a partir da junção de pequenas partes.

“I never am really satisfied that I understand anything; because, understand it well as I may, my comprehension can only be an infinitesimal fraction of all I want to understand about the many connections and relations which occur to me.”

(LOVELACE, Ada)

RESUMO

SAKAMOTO, Sarah Gomes. **Segurança, Privacidade e Blockchain no Contexto de Internet das Coisas**. 2020. 65 p. Monografia de Especialização em Internet das Coisas, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

A Internet das Coisas (IoT) transformou a indústria das telecomunicações, agregando áreas, ideias e tecnologias já existentes em um único conceito. Esse conjunto de objetos ou "coisas" conectadas à Internet, identificadas unicamente e que trabalham colaborativamente com um grau de inteligência, impõe diversos desafios quanto à implantação e provimento de recursos nessa infraestrutura. Nesse contexto, a segurança e a privacidade emergem como requisitos essenciais para esse campo de aplicações, trazendo com elas uma gama de desafios que necessitam ser discutidos e transpostos. Algumas soluções para essas questões são propostas na literatura, entre elas, o uso de blockchain, um novo paradigma que vai ao encontro dos principais problemas enfrentados em IoT. Este trabalho apresenta o contexto e os principais desafios considerando os requisitos de privacidade e segurança em Internet das Coisas, no âmbito tecnológico e jurídico. Adicionalmente, o tema é relacionado ao arcabouço jurídico brasileiro e são apresentadas algumas soluções para esses problemas. Por fim, algumas discussões a respeito do tema são levantadas.

Palavras-chave: Internet das Coisas. Privacidade. Segurança. Blockchain. LGPD.

ABSTRACT

SAKAMOTO, Sarah Gomes. **Security, Privacy and Blockchain in Internet of Everything Context**. 2020. 65 p. Monografia de Especialização em Internet das Coisas, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

Internet of Things transformed telecommunication industry and combined some application fields, ideas and already existing technologies into a single concept. This set of objects or "things" are connected to the Internet, uniquely identified, work collaboratively and provide some degree of intelligence. It imposes several challenges regarding the implantation and resources provision in this infrastructure. Under this context, security and privacy emerge as essential requirements, bringing many challenges that can be discussed and overcome. Some solutions are proposed in the literature, including the use of blockchain, a new paradigm that addresses the main problems faced in IoT. This work presents main challenges for privacy and security in the Internet of Everything context, under the the technological and legal perspective. Additionally, the issue is related to Brazilian legal framework and solutions to these problems are presented. Finally, we describe implications and discuss open questions about this overall topic.

Keywords: Internet of Things. Privacy. Security. Blockchain. LGPD.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

CF	Constituição Federal
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais

LISTA DE SIGLAS

6LoWPAN	*IPv6 over Low power Wireless Personal Area Networks*
BNDES	Banco Nacional de Desenvolvimento do Extremo Sul
CID	*Internet of Things*
CoAP	*Constrained Application Protocol*
DDoS	*Distributed Denial of Service*
DIKW	*Data, Information, Knowledge, Wisdom*
HTTP	*Hypertext Transfer Protocol*
IPv6	*Internet Protocol version 6*
IoT	*Internet of Things*
IoBT	*Internet of Battlefield Things*
IoMT	*Internet of Medical Things*
IoO	*Internet of Objects*
IoV	*Internet of Vehicles*
M2M	*Machine-to-Machine*
MAC	*Medium Access Control*
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
MQTT	*Messaging Queuing Telemetry Transport*
NIC	*National Intelligence Council*
OSI	*Open System Interconnection*
P2P	*Peer-to-Peer*
PHY	*Physical*
PKI	*Public Key Infrastructure*
RFID	*Radio-Frequency Identification*
RSSF	Redes de Sensores Sem Fio
SOA	*Service-Oriented Architecture*
WPAN	*Wireles Personal Area Networkds*

SUMÁRIO

1 INTRODUÇÃO

Décadas após a concepção de Weiser (1991), a computação ubíqua emerge como realidade. O imperativo tecnológico proporcionou mudanças profundas na sociedade, alterando a forma como os indivíduos interagem com os artefatos computacionais e como os sistemas estão dispostos nesse espaço cyber-físico. Como resultado dessa revolução, tem-se um modelo de computação no qual a tecnologia é transparente para o usuário, os dados são coletados no ambiente e processados colaborativamente, de forma eficiente e distribuída, e ainda, os dispositivos realizam ações e comunicam-se entre si através da rede. Esse paradigma é conhecido como Internet das Coisas (*Internet of Things* - IoT).

De acordo com a Cisco (2016), estima-se que 500 bilhões de objetos estarão conectados à Internet até 2030 e, em 2018, o número de dispositivos IoT já era maior do que a população mundial (YU *et al.*, 2018). Essa rede de objetos interconectados não realiza somente a captura de informações e interage com o mundo físico, como também usa os padrões existentes da Internet para prover serviços com uma vasta gama de aplicações. Segundo Mckinsey & Company (2019), o número de empresas que utilizam tecnologias IoT aumentou de 13% em 2014 para cerca de 25% em 2019 e a previsão é que o investimento nessas plataformas tenha um crescimento de 13,6% ao ano até 2022.

O cenário de utilização dessas aplicações permeia diversos domínios, desde saúde, gestão de serviços públicos, construção e cidades inteligentes até integridade da cadeia de suprimentos e agricultura. Todos esses objetos físicos e a infraestrutura de comunicação subjacente transformou a Internet, antes estática, em uma totalmente integrada (GUBBI *et al.*, 2013) e os espaços em ambientes inteligentes (RAJ; RAMAN, 2017).

A conectividade e a troca de dados, inclusive em tempo real, permite a implantação de novos recursos e a inteligência aplicada no processamento de um grande volume de dados traz facilidade, produtividade e diversos benefícios (HE *et al.*, 2016) para os usuários desse ecossistema.

No entanto, esse panorama levanta diversos desafios (CONTI *et al.*, 2018; ZARPELÃO *et al.*, 2017) quanto à privacidade e segurança, que tornam ainda mais relevante seu estudo ao considerar o impacto de vulnerabilidades nesse contexto, tendo em vista a infinidade de aplicações que tangem IoT e a sensibilidade dos

dados pessoais coletados e processados. E ainda, a preocupação com questões de privacidade e segurança é muitas vezes deixada em segundo plano devido à rápida evolução desse paradigma e aos desafios de desenvolvimento (CHIANG; ZHAND, 2016), associados à infraestrutura heterogênea e outras características intrínsecas. Essas questões, quando tratadas, devem considerar as particularidades que envolvem o ecossistema IoT.

Dentre algumas possíveis soluções para esses problemas surge blockchain, uma tecnologia que recebeu destaque recentemente por apresentar alternativas promissoras. Blockchain baseia-se em uma rede *Peer-to-Peer* (P2P) e provê segurança de maneira descentralizada e com uso de criptografia. Por serem ambas as tecnologias emergentes, a combinação Blockchain-IoT merece especial atenção e análise dentro desse cenário.

Considerando o exposto, este trabalho visa apresentar um estudo acerca de segurança, privacidade e blockchain no contexto de IoT. Os conceitos pertinentes a essa tríade são explorados e apresentados nos próximos capítulos.

1.1 OBJETIVOS

Nesta seção são apresentados os objetivos geral e específicos do trabalho, relativos ao problema anteriormente apresentado.

1.1.1 Objetivo Geral

O objetivo geral deste trabalho é apresentar um estudo sobre segurança e privacidade no contexto de Internet das Coisas.

1.1.2 Objetivos Específicos

Para isso, têm-se os seguintes objetivos específicos:

- Elicitar os principais desafios para segurança e privacidade em IoT;
- Apresentar o arcabouço jurídico brasileiro relacionado ao tema;
- Apresentar principais características de blockchain;

- Apresentar algumas soluções para os desafios apresentados, entre eles, blockchain;
- Analisar o contexto e identificar questões em aberto para pesquisas futuras.

1.2 ESTRUTURA DO TRABALHO

Esta monografia de especialização está dividida em 4 (quatro) seções. Nesta primeira seção foi introduzido o tema do trabalho, além de serem abordados a motivação e os objetivos geral e específicos da pesquisa.

Já na segunda seção: “Fundamentação Teórica”, serão apresentados os conceitos referentes à Internet das Coisas e Blockchain, visto que compõem a base teórica necessária para compreensão do tema.

A seguir na terceira seção: “Aspectos de Privacidade e Segurança em IoT”**,** serão abordados os riscos à privacidade, legislação referente à defesa desse direito, algumas soluções, dentre elas, o uso de blockchain, e, ainda, questões em aberto.

Por fim, serão apresentadas as conclusões deste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

A revolução tecnológica ocorrida nas últimas décadas destaca o papel de novas tendências, seus estudos e suas aplicações. Para o entendimento do contexto no qual este trabalho está inserido, faz-se necessário a apresentação de um referencial teórico. Nas seções seguintes serão apresentados os conceitos de Internet das Coisas e Blockchain.

2.1 INTERNET DAS COISAS

A crescente demanda por dispositivos na sociedade moderna é uma realidade. A tecnologia está inserida nas atividades mais simples, melhorando a qualidade de vida e trazendo eficiência na realização de várias atividades nos mais variados setores, de forma transparente. A comunicação com as máquinas e entre máquinas é inevitável, porém essa interação e novas tecnologias merecem especial atenção, devido aos impactos que promovem em todas as áreas.

Segundo estudo apoiado pelo BNDES em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) divulgado em 2018, a Internet das Coisas terá um impacto econômico de 4 a 11 trilhões de dólares no mundo até 2025. No Brasil, a estimativa é de 50 a 200 bilhões de dólares por ano.

Nesse cenário, torna-se necessário conceituar essa inovação e toda a infraestrutura associada a adoção dessa tendência. Nas próximas seções serão abordadas a definição de Internet das Coisas, suas áreas de aplicação, principais características e tecnologias associadas, além de inserir segurança nesse contexto.

2.1.1 Conceituação

A Internet das Coisas refere-se a uma rede de objetos interconectados, identificados unicamente, que se comunicam entre si e com outros sistemas, provendo uma gama de serviços. Esse conjunto de objetos ou "coisas" está conectado à Internet, possui capacidades de captura e compartilhamento de dados e pode ser usado para realização de tarefas complexas com um algo grau de inteligência (CONOSCENTI; VETRO; MARTIN, 2016; SETHI; SARANGI, 2017).

De acordo com Dorri, Kanhere e Jurdak (2016), IoT pode ser vista como uma evolução natural da Internet, que passa de uma rede de computadores para uma de sistemas embutidos e cyber-físicos. O termo foi originalmente proposto por Kevin Ashton em 1999 (ASHTON, 2009) e desde então, tem sido adotado na academia e na indústria nos mais diferentes contextos.

Diversos autores expõem definições acerca desse novo paradigma (ATZORI; IERA; MORABITO, 2010), destacando as capacidades de computação e rede embutidas em um único objeto (PEÑA-LÓPEZ *et al.*, 2005), a integração entre os objetos em uma rede de informação (ZHANG *et al.*, 2014), a presença pervasiva desses elementos com a cooperação entre seus vizinhos (GIUSTO *et al.*, 2010) e a interação entre o mundo digital e o físico com o uso de sensores e atuadores (VERMESAN *et al.*, 2011).

A participação ativa dos objetos no processo de negócio também é outra característica dessas redes, tendo que vista que são capazes de atuar e reagir a determinados eventos e situações no ambiente em que se encontram (MADAKAM *et al.*, 2015), devido às capacidades autonômicas e de inteligência, resultantes da aplicação das diversas tecnologias nesse sistema.

Segundo Witkowski (2017), três conceitos distintos estão relacionados à IoT: contexto, onipresença e otimização. Contexto refere-se à ciência de informações, tais como condição física, localização ou condições atmosféricas pelo objeto; Onipresença é trazida pela ubiquidade, em que bilhões de objetos estão espalhados pelo ambiente físico; A otimização está ligada à ideia de interação do objeto com o ambiente e sua resposta imediata, ocasionando uma mudança de estado ou uma ação.

Devido a essas características, alguns domínios são especialmente beneficiados por soluções propostas nesses cenários para problemas recorrentes. Dentre esses domínios, também chamados de verticais de IoT (CONDOLUCI *et al.*, 2018), pode-se citar saúde, cidades inteligentes, controle e medição de sistemas, integridade da cadeia de suprimentos e agricultura. Como exemplos de aplicações desses cenários, tem-se, no domínio da saúde, a detecção de quedas de pessoas idosas (MANO *et al.*, 2016), sistemas de monitoramento de saúde vestível e de redes de corpo humano (BSNs) (YANG *et al.*, 2014; YEH, 2016), além de hospitais inteligentes (YU; LU; ZHU, 2012).

Já no âmbito de cidades inteligentes, há trabalhos na linha de casas inteligentes (ALAA *et al.*, 2017), monitoramento da qualidade do ar e de barulho (ZANELLA *et al.*, 2014), gerenciamento de energia (EJAZ *et al.*, 2017) e, ainda, de otimização de tráfego, tais como o monitoramento em tempo real do tráfego para prevenção de congestionamentos (THAKUR *et al.*, 2016) e utilização de rotas baseadas em grupo (SANG *et al.*, 2017).

Na vertical da indústria, na subárea de transporte e logística, há a questão da cadeia de suprimentos, que inclui soluções de rastreio de produtos, tais como o de Abad *et al.* (2010) e Tian (2017). Outros temas ainda permeiam a combinação de algumas verticais, possibilitando uma variedade de aplicações.

Podem-se citar três tipos de interações nas aplicações deste campo de pesquisa: (a) entre pessoas (*people-to-people*), (b) entre pessoas e objetos e (c) entre objetos (*things-to-things*). Considerando que existem relações entre objetos e pessoas, é importante considerar fatores éticos e legais considerando esse contexto.

Além do termo IoT, outras denominações (BANERJEE; LEE; CHOO, 2018) também se relacionam a esse conceito, tais como Internet de todas as coisas (*Internet of Everything*), Internet das coisas médicas (IoMT - *Internet of Medical Things*), Internet das coisas militares (IoBT - *Internet of Battlefield Things*), Internet dos veículos (IoV - Internet of Vehicles) e Internet dos objetos (IoO - *Internet of Objects*). Apesar desses termos serem relativamente recentes, conceitos correlatos que foram agregados pela Internet das Coisas já possuem décadas de existência.

Um exemplo é a área de sistemas de monitoramento e controle. Desde a década de 70 que sistemas desse tipo são propostos e desenvolvidos, utilizando as redes de comunicação existentes e diversas tecnologias para acesso remoto, dando origem posteriormente a termos, tais como comunicação "*Machine-to-Machine*" (M2M). M2M (KIM *et al.*, 2013) refere-se à comunicação direta entre dispositivos que são utilizados para monitorar determinado evento no ambiente. Conforme visto anteriormente, IoT incorpora interação entre objetos (*things-to-things* ou M2M) além das outras formas de interação.

Outro termo que também intercepta IoT é Rede de Sensores Sem Fio (RSSF). RSSFs são redes constituídas de diversos dispositivos de tamanho reduzido denominados "nós", equipados com sensores de baixo custo e que são colocados em um ambiente de forma *ad hoc* para realizar sensoriamento, processamento e transmissão de dados. Esse tipo de rede é caracterizado por atuar

de forma colaborativa e possuir limitações quanto aos recursos de memória, processamento e energia.

Os nós se comunicam com o gateway, que geralmente é responsável pela comunicação com o servidor que fará o tratamento desses dados, e também pode haver comunicação entre dispositivos, com uma topologia de múltiplos saltos. Tendo em vista as limitações dessas redes, principalmente no tocante à eficiência energética, diversas tecnologias de transmissão, protocolos de comunicação e esquemas de desligamento e controle de topologia são propostos para fins de otimização do consumo de bateria.

Como os nós sensores são projetados para atuarem no ambiente sem intervenção humana, faz-se necessário que a rede possua mecanismos de adaptação e auto reconfiguração, de forma a acomodar mudanças durante sua operação (DELICATO, 2005). Assim como M2M, surgiu antes de IoT, na década de 80, e foi inicialmente denominado rede de sensores distribuídos; somente após alguns anos de desenvolvimento da área tornou-se RSSF.

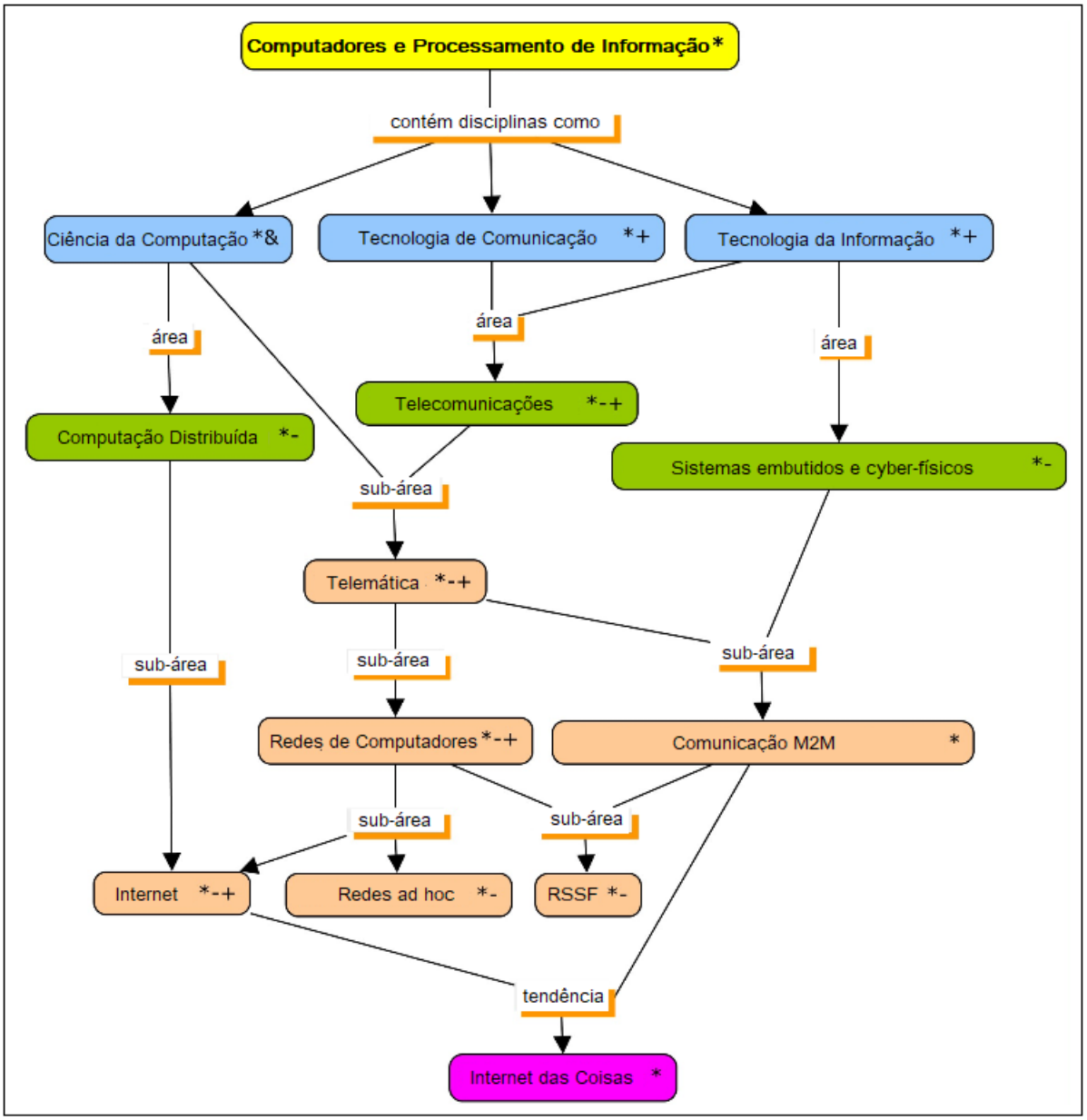
Manrique, Rueda-Rueda e Portocarrero (2016) abordam em seu trabalho uma análise da relação entre Internet das Coisas e Redes de Sensores Sem Fio. Entre suas contribuições, apresenta um mapa conceitual relacionando ambos os termos, organizado hierarquicamente através da análise do tesauro proposto pelo IEEE, ACM e UNESCO. No mapa, ilustrado na Figura 1, é possível verificar o relacionamento entre os conceitos, inclusive, M2M, e conclui-se que tanto IoT quanto RSSFs são influenciados por M2M, mas possuem origens um pouco distintas. Outra diferença que tem impactos no mapa é que IoT faz uso da Internet, enquanto que RSSFs podem utilizar a Intenet, mas não estão necessariamente conectadas a ela.

O trabalho ainda apresenta uma comparação entre os requisitos de aplicação quanto ao grau de relevância de cada um dos domínios, conforme ilustrado na Tabela 1. Os valores dos graus representados são alto, médio, baixo ou nulo. Diante do exposto, é possível verificar que segurança e privacidade possuem maior relevância no contexto de IoT do que em RSSF, assim como outros requisitos, tais como escalabilidade, qualidade de serviço, heterogeneidade, mobilidade, processamento de dados e identificação dos objetos.

Então, apesar dos termos possuírem muitas sobreposições entre domínios e aplicações, IoT é um termo mais amplo, que utiliza diversas tecnologias para prover

as ideias propostas, tais como uso da Internet, utilização de IPv6 para identificação única de cada um dos dispositivos, computação em nuvem, Big Data, inteligência artificial, *Radio-Frequency IDentification* (RFID) e RSSF.

Figura 1 – Mapa conceitual baseado no tesauro do relacionamento entre RSSF e IoT



Fonte: Adaptado (traduzido) de Manrique, Rueda-Rueda e Portocarrero (2016).

Apesar de IoT não possuir nenhuma tecnologia fundamentalmente obrigatória, atualmente, tem as Redes de Sensores Sem Fio como um de seus principais componentes. Por isso, ao ver a descrição de RSSF pode-se notar diversas características que são de IoT, o que gera uma falsa ideia de que possuem o mesmo significado.

Tabela 1 – Relevância dos requisitos de aplicação entre IoT e RSSF

Requisito	RSSF	IoT
Segurança e Privacidade	Médio	Alto
Robustez	Alto	Alto
Escalabilidade	Médio	Alto
Qualidade de Serviço	Médio	Alto
Heterogeneidade	Médio	Alto
Implantação e Cobertura	Alto	Nulo
Mobilidade	Médio	Alto
Energia / Gerenciamento de Energia	Alto	Médio
Identificação das Coisas	Nulo	Alto
Autonomia	Alto	Alto
Processamento de Dados	Nulo	Alto
Comunicação e Conexão à Internet	Alto	Alto

Fonte: Manrique, Rueda-Rueda e Portocarrero (2016).

Passada essa conceituação, a seguir, serão apresentadas algumas características de Internet das Coisas, com o detalhamento de algumas tecnologias utilizadas e algumas propriedades intrínsecas presentes nessas redes.

2.1.2 Características

Como foi abordado na seção anterior, a Internet das Coisas baseia-se nessa rede distribuída de dispositivos comunicando-se através de uma infraestrutura heterogênea, de forma autônoma, colaborativa e autoconfigurável, provendo funcionalidade e serviços de forma inteligente.

Diversas características das Redes de Sensores Sem Fio são também de Internet das Coisas, como a descentralização e os recursos limitados. Sha *et al.* (2018) fazem uma comparação entre as características de RSSF e IoT quanto ao acoplamento físico, comunicação, limitações, diversidade, escalabilidade e privacidade. Desse comparativo, podem-se extrair as principais características de IoT: alto acoplamento, comunicação em duas direções, limitação em recursos de armazenamento, processamento e energia, escalabilidade extremamente alta e privacidade como uma expectativa realmente alta.

Em IoT, os dispositivos são identificados unicamente na rede global e, para isso, é utilizado o IPv6. O IPv6 (*Internet Protocol version 6*) utiliza 8 grupos de 4

dígitos hexadecimais, permitindo um endereçamento de aproximadamente $3.4x10^{38}$ de endereços válidos, o que comporta o endereçamento necessário e apoia a escalabilidade da rede em questão de identificação dos seus componentes.

O ecossistema IoT envolve uma gama de objetos com tecnologias de comunicação e operação diferentes, conforme mostra a Figura 2. Em geral, organiza-se a infraestrutura de IoT de acordo com as camadas do modelo OSI e os padrões utilizados buscam aproveitar as características intrínsecas citadas para maximizar a eficiência. A seguir, serão listadas algumas tecnologias e protocolos utilizados nessas redes, seguindo tal estruturação.

Nas camadas física e enlace podem-se citar os padrões 802.15.4 e 802.15.4e, que atuam nas camadas 1 e 2 e visam suprir as necessidades de baixa transmissão de dados e otimização de recursos. Eles permitem redes com múltiplos nós, o que não era suportado pelo padrão 802.15.1 (*Bluetooth*), por exemplo. Quanto à segurança, vale ressaltar que é possível utilizar o bit de habilitação de segurança (*Security Enabled Bit*) no campo de controle de frame no header do MAC 802.15.4 para segurança. O 802.15.4e surge para preencher lacunas ainda deixadas pelo 802.15.4, tais como baixa confiabilidade na comunicação e pouca proteção contra desvanecimento e interferências. Todos esses padrões estão relacionados às WPANs (*Wireless Personal Area Networks*).

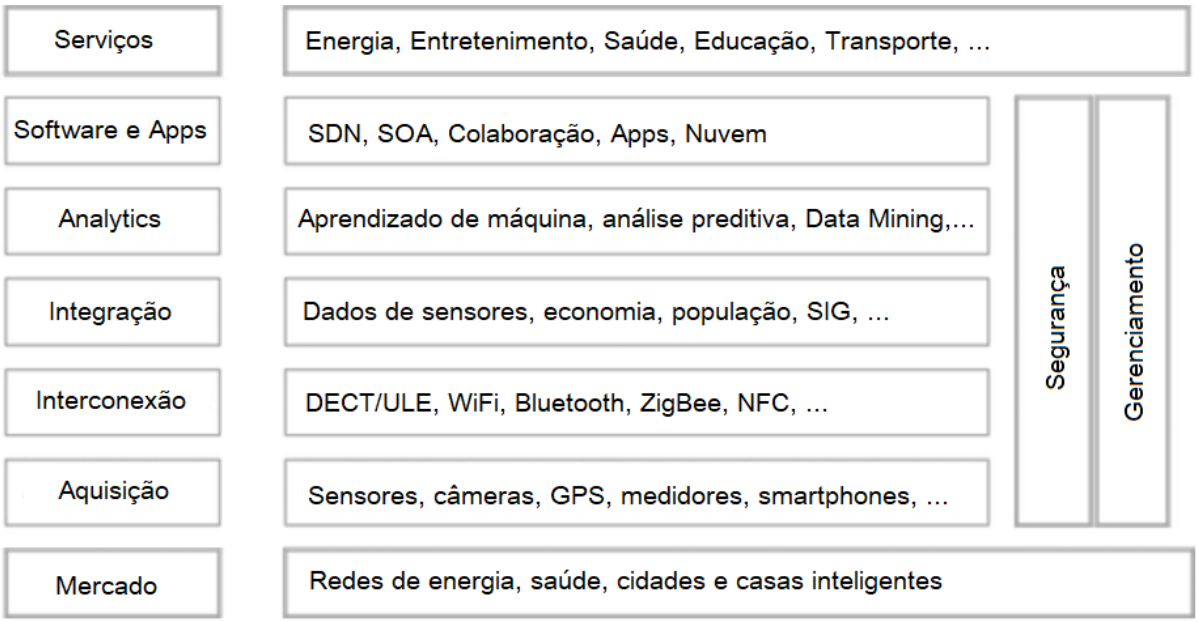
Outro protocolo utilizado em IoT é o *IPv6 over Low power Wireless Personal Area Networks* (6LoWPAN), um protocolo intermediário entre a camada de rede e as camadas PHY/MAC, que permite a utilização do protocolo IPv6 sobre o protocolo 802.15.4, visto que comprime e fragmenta os *headers* dos pacotes IPv6.

Para roteamento, ou seja, referente à camada de rede, tem-se o *Routing Protocol for Low power and Lossy Networks* (RPL). O RPL fornece um nível de segurança utilizando o campo “segurança” depois do *header* ICMPv6 de 4 bytes. Além do RPL, existem outros protocolos, tais como *COgnitive RLP* (CORPL) e *Channel-Aware Routing Protocol* (CARP), projetados para redes específicas.

Na camada de transporte são utilizados o *User Datagram Protocol* (UDP) e *Transmission Control Protocol* (TCP). O TCP fornece confiabilidade na entrega dos pacotes, controle de fluxo e entrega ordenada de pacotes. Além disso, é possível estabelecer conexão através do *handshake* triplo, e realiza retransmissão em caso de perda de dados. Já o UDP não fornece não é orientado a conexão, não fornece confiabilidade e controle de fluxo, além de realizar reagrupamento de dados de

forma não ordenada. Porém, fornece menor overhead na transmissão, com um cabeçalho menor se comparado ao TCP.

Figura 2 – Ecossistema IoT



Fonte: Adaptado de Salman e Jain (2015).

Nas camadas superiores, os principais protocolos são o *Messaging Queuing Telemetry Transport* (MQTT) e *Constrained Application Protocol* (CoAP). O CoAP utiliza o UDP, provê uma interface *RESTful* e possui um funcionamento semelhante ao *Hypertext Transfer Protocol* (HTTP). O MQTT utiliza TCP na camada inferior, contando, assim, com confiabilidade e utiliza um sistema de mensagens baseado no sistema de publicação e subscrição (*publish/subscribe*) com comunicação intermediada por um *broker*. Também há outros protocolos, tais como o *MQTT for Sensor Networks* (MQTT-SN) e o *Secure MQTT* (SMQTT). O MQTT-SN baseia-se no MQTT, porém com algumas modificações para otimização de recursos restritos, como o uso do protocolo UDP, e o SMQTT utiliza criptografia para aumentar a segurança.

Um projeto IoT deve levar em consideração os requisitos da aplicação final para escolha da tecnologia associada que fundamentará a estrutura desse sistema. De acordo com Sommerville (2011), requisito é a descrição do sistema, com suas funções e restrições (RFs e RNFS - requisitos funcionais e não funcionais) que são gerados durante o processo da construção da solução proposta.

Um projeto IoT, em geral, não envolve somente o desenvolvimento de um software. O projeto baseia-se no desenvolvimento de uma solução considerando aspectos físicos e lógicos, com toda uma infraestrutura de rede subjacente. A escolha da tecnologia geralmente envolve o hardware, com as características físicas, tais como sensores, atuadores, processador, memória, antenas de comunicação, caso sejam separados, ou do *kit* de desenvolvimento, os protocolos de comunicação, e os recursos a nível de aplicação.

Isso impõe diversos desafios para os projetistas desses sistemas, que devem delinear os aspectos humanos de interação com os usuários (*e.g*. como será realizada a coleta e o sensoriamento de dados no ambiente, como será a resposta do sistema para o mundo externo, de que forma a ubiquidade será provida), identificando os requisitos de alto-nível do sistema de acordo com as funcionalidades desejadas e, somente em seguida, tomar decisões acerca da escolha das tecnologias de comunicação associadas.

Por exemplo, se o sistema proposto considerar baixa transmissão de dados, o uso de alguns protocolos pode ser mais apropriado do que a escolha de outros. Se a eficiência energética for um fator crítico, a escolha do hardware como também dos protocolos de comunicação pode fazer toda a diferença no desenvolvimento e desempenho do sistema.

Baseado nessa linha, Da Xu, He e Li (2014) apresentam um conjunto de considerações de projeto para aplicações IoT da perspectiva técnica, de forma que as decisões de projeto e da tecnologia atendam as demandas levantadas com essas perguntas. As considerações estão reunidas na Tabela 2.

Tabela 2 – Considerações de projeto para aplicações IoT

Meta de projeto	Descrição
Energia	Por quanto tempo o dispositivos IoT operará com uma fonte de energia limitada?
Latência	Quanto tempo é necessário para propagação e processamento da mensagem?
Throughput	Qual é o volume máximo de dados que pode ser transportado pela rede?
Escalabilidade	Quantos dispositivos são suportados?
Topologia	Quem precisa de comunicar com quem?
Segurança	Quão segura é a aplicação?

Fonte: Da Xu, He e Li (2014).

Da Xu, He e Li (2014) ainda descreve a infraestrutura subjacente de IoT como uma arquitetura SOA de quatro camadas, conforme ilustrado na Figura 3: (a) camada de sensoriamento, que se encontra integrada ao hardware existente e realiza o sensoriamento e o controle do mundo físico; (b) camada de rede, que provê suporte de rede básicos e transferência de dados; (c) camada de serviço, responsável pela criação e gerenciamento dos serviços; (d) camada de interface, que realiza interação com os usuários e outras aplicações.

Figura 3 – Arquitetura SOA de IoT

Fonte: Autoria própria, representação da proposta de Da Xu, He e Li (2014).

As principais características de IoT que impõem desafios ao desenvolvimento de novas soluções e à segurança e à privacidade são as seguintes: (a) pluralidade e heterogeneidade de dispositivos, (b) descentralização, (c) escalabilidade, (d) recursos limitados (processamento, armazenamento, energia), (e) grande volume de dados.

A pluralidade de dispositivos é marcada pela presença de diferentes hardwares e sistemas embarcados, com interfaces distintas que variam desde interfaces físicas simples com sensores de baixo custo até aplicações na nuvem. Essa heterogeneidade fornece uma múltipla superfície de ataque. A falta de um padrão de autenticação e autorização aumenta os desafios inerentes a essas características. Somado a isso, tem-se a descentralização, que dificulta o gerenciamento da rede de forma segura.

A natureza das aplicações IoT que envolvem a alta pervasividade, o grande volume de dados e a junção de dados de diferentes contextos elevam a importância da privacidade, conforme mencionado anteriormente. E ainda, técnicas para melhorar a segurança geralmente envolvem criptografia, que exige maior poder de processamento. No entanto, a característica de recursos limitados impõe mais um desafio.

2.1.3 Segurança

A Segurança da informação baseia-se em proteger ativos (informação e sistemas de informação) de acesso, uso, divulgação, perturbação, modificação ou destruição indevidos ou não autorizados (SATTAROVA; KIM, 2007). Ela é fundamentada em 3 princípios basilares, conhecidos como “tríade CID” ou “*CIA Triad”*, que são: (a) confidencialidade, (b) integridade e (c) disponibilidade.

A confidencialidade é garantir o acesso somente a pessoas autorizadas; a integridade refere-se à salvaguarda da exatidão e completeza da informação, ou seja, a garantia de que não sofreu modificações durante o armazenamento ou a transmissão e recepção; a disponibilidade refere-se à garantia de acesso ao ativo sempre que solicitada por um requisitante legítimo.

Outros conceitos também estão relacionados à segurança e citados como princípios adicionais, entre eles estão a autenticidade, que garante a identidade de quem realiza a operação, ou seja, a o indivíduo é quem diz ser, e o não repúdio, que visa garantir que a autoria da operação não poderá ser negada.

É perceptível a transformação causada pela adoção de IoT em diversos aspectos, seja no comércio, na comunidade global e na vida pessoal dos indivíduos. A Internet das Coisas já foi elencada pelo Conselho Nacional de Inteligência dos Estados Unidos como uma das seis tecnologias civis disruptivas com impactos potenciais nos interesses da nação até 2025. Porém, como citado na publicação, assim como essa tecnologia traz oportunidades, também apresenta diversos riscos à segurança, advindos do controle, localização e monitoramento remoto, distribuindo esses riscos de forma mais ampla do que a Internet já é capaz de fazer atualmente.

Segundo o Relatório Global de Riscos do Fórum Econômico Mundial de 2020 (WEF, 2020), os ataques cibernéticos são um dos dez maiores riscos levantados para a próxima década, com impacto profundo em diversas esferas. Ataques cibernéticos em larga escala são vistos como riscos à quebra de redes e infraestruturas de comunicação em escala mundial. Ataques DDoS (*Distributed-Denial-of-Service*), tal como o ocorrido em 2016 pela *botnet* Mirai e a propagação do *ransomware* WannaCry no ano seguinte são exemplos do impacto que grandes ataques podem causar.

Em toda a gama de aplicações é nítida a sensibilidade de diversos tipos dados, além do grau de envolvimento dessa tecnologia com aspectos relevantes da

vida pessoal dos usuários. Ao analisarmos alguns exemplos de aplicações citados na seção 2.1.1, podem-se destacar dados médicos, de deslocamento de indivíduos, de rastreio no transporte de mercadorias e de informações residenciais. Vale ressaltar que os objetos de uma solução IoT não somente coletam informações pessoais, como também monitoram as atividades dos usuários, tais como movimentos, hábitos e interações (YANG *et al.*, 2017; SICARI *et al.*, 2015). Considerando o exposto, se esses dados forem divulgados inapropriadamente ou caso tenham um fim diverso, podem colocar em risco o negócio de uma empresa, a imagem e a honra de um paciente e até a vida de pessoas.

Considerando as limitações presentes nos equipamentos IoT e a heterogeneidade das plataformas que compõem a rede, Khan e Salah (2018) apresentam uma taxonomia de problemas relacionados à segurança em IoT, ilustrada no Quadro 1, categorizando as ameaças de segurança de acordo com três níveis distintos: (a) baixo-nível, (b) nível intermediário e (c) alto-nível.

As ameaças de baixo-nível referem-se a problemas de segurança relacionados à camada física e enlace, além de questões de hardware. Nessa categoria estão ataques como *jamming*, inicialização insegura, ataques *sybil* e *spoofing* de baixo-nível, interface física insegura e privação de sono.

Por exemplo, ataques *sybil* caracterizam-se por nós maliciosos utilizarem identidade falsa para degradarem recursos da rede IoT. No ataque *sybil* de baixo-nível, o nó pode utilizar um endereço MAC falso e, nós legítimos podem perder acesso a recursos da rede. Já os ataques de privação de sono aproveitam-se de dispositivos com recursos limitados de energia e fazem com que os nós fiquem ligados e gastem sua energia, sem a real necessidade.

Ameaças de nível intermediário estão associadas à comunicação, roteamento e gerenciamento de sessão, referindo-se às camadas de rede e transporte. Um exemplo de ataque nessa categoria é a reserva de *buffer*. O atacante aproveita-se do fato que um nó necessita reservar um espaço do buffer para remontar os pacotes recebidos e, então, envia pacotes incompletos, o que ocasiona um DoS (*Denial-of-Service*), visto que outros pacotes legítimos serão descartados.

Quadro 1 – Taxonomia de ameaças à segurança em IoT

Categoria	Problema
Baixo Nível	*Jamming*
	Inicialização insegura
	Sybil e *spoofing* de baixo-nível
	Interface física insegura
	Privação de sono
Nível Intermediário	Ataque de repetição ou duplicação devido à fragmentação
	Descoberta de vizinhos insegura
	Reserva de *buffer*
	Ataque de roteamento RPL
	Ataques Sinkhole e Wormhole
	Sybil de camada intermediária
	Autenticação e comunicação segura
	Segurança ponta-a-ponta a nível de transporte
	Estabelecimento de sessão e retomada
	Violação de privacidade em nuvem baseada em IoT
Alto-Nível	Segurança CoAP com Internet
	Interfaces inseguras
	Software / Firmware inseguro
	Segurança de middleware

Fonte: Khan e Salah (2018).

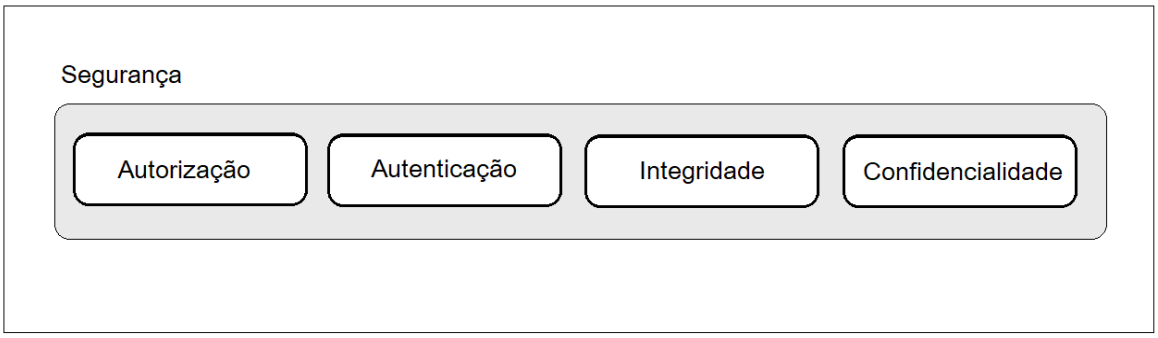
Outro exemplo é o ataque *sinkhole*, no qual o nó malicioso responde a requisições de roteamento, fazendo com que os pacotes passem por ele, e aproveita-se disso para realizar as atividades maliciosas na rede. Outro tipo de ataque é a repetição ou duplicação devido à fragmentação, que se aproveita da fragmentação de pacotes IPv6 exigida por dispositivos que usam 802.15.4 e, então, o atacante envia pacotes IPv6 duplicados, o que irá afetar a remontagem dos pacotes e, portanto, dificultando o processamento de pacotes legítimos.

Já as ameaças de alto-nível incluem aquelas relacionadas a nível de aplicação. Por exemplo, interfaces inseguras envolve a vulnerabilidade de interfaces *web*, de aplicações móveis e em nuvem, que podem afetar a privacidade dos dados; segurança de middleware envolve a ameaça em aplicações que utilizam middleware em sua infraestrutura para realizar comunicação com diversas entidades heterogêneas e que, por isso, necessitam prover uma comunicação segura.

Considerando esse contexto, Singh e Singh (2015) identificaram alguns desafios relacionados à segurança em Internet das Coisas, dentre eles estão a segurança e a privacidade dos dados, a falta de padrões comuns e questões técnicas. Posteriormente, Elkhodr, Shahrestani e Cheung (2016) apontam mais desafios de segurança em IoT, que incluem: segurança ponta-a-ponta, gerenciamento de acesso e identidade, controle de acesso e *compliance*.

Baseado nos desafios elencados, eles identificaram quatro principais requisitos de segurança em IoT, conforme ilustrado na Figura 4: (a) autorização, (b) autenticação, (c) integridade e (d) confidencialidade.

Figura 4 – Requisitos de segurança



Fonte: Autoria própria.

Para uma comunicação segura, esses requisitos necessitam ser atendidos. Faz-se necessário a adoção de mecanismos de autorização para garantir o acesso aos recursos e serviços somente a elementos autorizados, como também autenticação entre as duas partes da comunicação. A integridade dos dados, ou seja, a garantia de que os dados estão intactos (LIU *et al.*, 2015), precisa ser mantida, assim como a confidencialidade, mesmo com o grande volume e distribuição dos dados, além da descentralização da rede.

2.2 BLOCKCHAIN

Blockchain é uma tecnologia emergente que revolucionou o cenário mundial. Proposta surgida em 2008 com a publicação do *white paper* "*Bitcoin: A Peer-to-Peer Electronic Cash System*", esse fenômeno se popularizou com a criação da criptomoeda Bitcoin por Nakamoto *et al.* (2008). O bloco gênesis, ou seja, o primeiro

bloco da rede foi criado no início do ano seguinte à publicação e, desde então, expandiu-se em uma escala sem precedentes.

Nesta seção será apresentado o termo blockchain, juntamente com suas principais características, alguns conceitos correlatos e princípios básicos de seu funcionamento.

2.2.1 Conceitos e Funcionamento

Blockchain ou cadeira de blocos consiste em uma base de dados descentralizada e distribuída, que permite manter registros de forma imutável e inviolável, fornecendo robustez, segurança e transparência. Criptografia é utilizada para encadear os blocos, formando uma rede *Peer-to-Peer* (P2P) que mantém esses registros.

Mougayar (2017) traz definições distintas para o termo blockchain sob três perspectivas: (a) técnica, (b) corporativa e (c) legal. Essas definições são trazidas no Quadro 2.

Quadro 2 – Definições de blockchain sob diferentes perspectivas

Perspectiva	Definição
1. Técnica	Base de dados de *back-end* que mantém um registro distribuído abertamente.
2. Corporativa	Rede de trocas para valores em movimento entre partes.
3. Legal	Um mecanismo de validação de transações que não requer apoio de intermediários.

Fonte: Adaptado de Mougayar (2017).

Ela é uma mudança de paradigma ainda em curso, pois propõe uma nova forma de realizar transações que desafiam modelos já estabelecidos e há anos existentes. A principal inovação trazida pela blockchain é o fornecimento de confiança sem a necessidade de uma organização central, o que traz uma série de implicações.

Confiança pode ser definida como um sentimento relacionado à segurança. Sob a ótica humana, a confiança refere-se à satisfação de uma expectativa, em geral, obtida através de informações necessárias para realizar de interações (ALBUQUERQUE, 2008). Sob a ótica computacional, confiança pode ser definida como “um nível particular de probabilidade subjetiva, na qual um agente acredita que

outro agente realizará uma ação em particular, que está sujeita a uma verificação e que influencia na própria ação do agente em si" (ALBUQUERQUE, 2008).

Os modelos atuais de confiança são baseados em uma entidade confiável que centraliza esse conceito. Um exemplo na esfera social é o controle de transações financeiras, que são regidas por normas estabelecidas e dependem de instituições bancárias, que realizam as transações entre os clientes e atuam como um intermediário entre eles. Outros exemplos incluem os governos, que se colocam como um ponto de controle e autoridade de confiança. Ainda pode-se citar os cartórios, que atuam como intermediários entre duas partes que desejam realizar uma transação e firmam um acordo através de um contrato.

Na computação, um exemplo do modelo centralizado é a infraestrutura de chave pública (ICP ou PKI - *Public Key Infrastructure*), que suporta a utilização de criptografia assimétrica. Esse sistema baseia-se em dois componentes: (a) autoridade certificadora e (b) certificado digital. O certificado digital é o documento que identifica de forma segura e inequívoca uma pessoa física ou jurídica. Já a autoridade certificadora é a entidade responsável pela emissão desse documento. Ela é a retratação da autoridade de confiança citada anteriormente.

O problema desse modelo é a dependência do ator centralizador, responsável por garantir a confiança do sistema. Blockchain proporciona uma quebra de paradigma ao trazer essa camada de confiança em um modelo distribuído, permitindo que ativos sejam transferidos de forma direta, confiável e segura

Cada participante da rede possui uma cópia da base de dados, que são continuamente atualizadas e validadas. Por ser uma rede P2P e, portanto, possuir uma natureza distribuída, não é controlada por uma entidade central e não possui um único ponto de falha (SAGHIRI *et al.*, 2018).

O conceito de criptografia assimétrica também é uma das bases desse conceito. A identificação dos usuários de uma blockchain são definidas por um par de chaves criptográficas (uma privada e uma pública). A chave privada é utilizada para assinar as transações na rede, enquanto a chave pública representará o usuário, no caso, por exemplo, do Bitcoin, representa a carteira do usuário. Isso permite o anonimato, trazendo privacidade para a rede.

Seu funcionamento é baseado em alguns elementos: (a) transação, (b) bloco, (c) livro-razão, (d) *hash*, (e) minerador. Transações são as ações criadas pelos participantes do sistema. Pode ser uma troca, uma transferência bancária ou

qualquer outro tipo de informação que será registrada no sistema (BANAFA, 2017). Essas transações são gravadas em blocos e, para um bloco ser inserido na cadeia, necessita ser validado.

Livro razão ou *ledger* é esse conjunto de blocos que formam a cadeia, onde são feitos os registros das transações que constituem a base de dados da blockchain. Essa base de dados pública e distribuída pode ser acessada por todos os usuários.

Uma vez que a informação é inserida em um bloco e este bloco é validado e encadeado à rede, não será mais modificada; apenas novas informações são adicionadas. Cada bloco é feito a partir de informações do bloco anterior e possui um hash, atuando como *links* entre blocos anteriores. A hash garante a integridade da informação, sem ter que analisar todos os dados. Todo o histórico de transações fica armazenado no livro-razão e, por isso, esse registro é tido como imutável.

A validação dos blocos ocorre pelo processo de mineração. Os mineradores são entidades responsáveis por resolver problemas matemáticos complexos de alto custo de recursos computacionais. O processo de resolução desses problemas depende do algoritmo de consenso utilizado, dentre os mais famosos estão o *Proof-of-Work* e o *Proof-of-Stake*.

2.2.2 Consenso Distribuído

Como não existe uma entidade central para decidir o que é ou não válido para inserção na cadeia de blocos, a estratégia utilizada pela tecnologia blockchain é o consenso distribuído. Questão presente em sistemas distribuídos, o consenso está intimamente relacionado à capacidade de resolver problemas e a tolerância a falhas.

A ideia do consenso distribuído baseia-se no Problema dos Generais Bizantinos (*Byzantine Fault Tolerance*), o qual descreve a situação de um grupo de generais que precisa realizar um ataque em conjunto para conquistar uma cidade. Esse ataque necessita ser em conjunto, com todos os generais atacando ao mesmo tempo. Porém, nem todos os generais são confiáveis, ou seja, há generais maliciosos na rede. Ao receber um comando para esperar ou atacar, cada general deve transmitir essa informação aos generais mais próximos a ele. No final, deve haver um consenso sobre o ataque.

Diversos trabalhos na literatura propuseram soluções para resolver esse problema na área de sistemas distribuídos, com diversos algoritmos denominados algoritmos de consenso distribuído.

Alguns algoritmos de consenso distribuído são: *Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, Leased Proof-Of-Stake, Proof of Elapsed Time, Practical Byzantine Fault Tolerance, Simplified Byzantine Fault Tolerance, Delegated Byzantine Fault Tolerance, Directed Acyclic Graphs, Proof-of-Activity, Proof-of-Importance, Proof-of-Capacity, Proof-of-Burn e Proof-of-Weight*.

2.2.3 Tipos de Blockchain

As blockchains podem ser classificadas de acordo com o tipo de acesso aos dados e participação no processo de validação de um bloco à cadeia. Quanto ao tipo de acesso, pode ser: (a) pública, que é baseada em uma rede pública, ou seja, qualquer usuário pode fazer parte da rede ou (b) privada, que é restrita, ou seja, somente alguns usuários podem participar.

Quanto à participação no processo de validação dos blocos, pode ser: (a) com permissionamento ou (b) sem permissionamento. Na primeira, qualquer usuário pode ser um validador ou minerador, enquanto que na segunda (sem permissionamento), apenas alguns usuários poder ter tal atuação (MACHADO, 2018).

Apesar da tecnologia blockchain ser comumente referenciada pela rede Bitcoin ou ligada às criptomoedas, diversas redes foram propostas e são utilizadas nos dias atuais, para os mais variados cenários. Exemplos de blockchain públicas e sem permissionamento são Bitcoin e Ethereum, enquanto que Hyperledger e Ripple são com permissionamento (CHICARINO *et al.*, 2017).

Algumas blockchains também utilizam o conceito de contratos inteligentes ou *smart contracts*, que são *scripts* auto executáveis que residem dentro de uma blockchain (CHRISTIDIS; DEVETSIKIOTIS, 2016). Portanto, poderiam ser categorizadas de acordo com ou sem esse recurso, porém não é uma classificação comumente adotada. A blockchain mais popular que permite a criação de contratos inteligentes é a Ethereum, que possui a linguagem de programação *Solidity* para a definição desses contratos.

Dias (2019) apresenta uma análise comparativa entre as principais tecnologias ou plataforma de blockchain, como são referenciadas no trabalho. Nesse comparativo, apresentado na Figura 5, constam os domínios de aplicação de cada plataforma, a classificação quanto ao permissionamento, o algoritmo de consenso utilizado, a linguagem utilizada para o desenvolvimento de contrato inteligente (ou *smart contract*), caso se aplique, o ambiente de execução do contrato inteligente, modelo de dados e o nome da criptomoeda, caso se aplique.

Figura 5 – Comparação entre diversas tecnologias blockchain

Plataforma	Domínio	Tipo de *blockchain*	Mecanismos de consenso	*Smart contracts*	Ambiente de execução de *smart contracts*	Modelo de dados	Cripto moeda
Bitcoin	Cripto moeda	Sem permissões	PoW	–	–	UTXO	BTC
Ethereum	Aplicações descentralizadas Cripto moeda	Sem permissões	PoW	Solidity	EVM	Conta de utilizador	ETH
Quorum	Múltiplos setores	Com permissões	Raft IBFT	Solidity	EVM	Conta de utilizador	–
Hyperledger Fabric	Múltiplos setores	Com permissões	Framework conectável	Java Node.js Go	Dockers	Conta de utilizador	–
Corda	Serviços financeiros	Com permissões	Framework conectável	Java Kotlin	JVM	UTXO	–
Ripple	Cripto moeda	Com permissões	Sistema de votos probabilísticos	–	–	UTXO	XRP
Tezos	Aplicações descentralizadas Cripto moeda	Sem permissões	PoS	Michelson	Dockers	Conta de utilizador	Tezos
BigchainDB	Múltiplos setores	Com permissões	Tendermint	–	–	Conta de utilizador	–

Fonte: Dias (2019).

Outra tecnologa popularmente conhecida como uma blockchain é IOTA, criada em 2015 para pagamentos no universo de Internet das Coisas, porém é uma estrutura de dados baseada no uso de *Directed Acyclic Graph* (DAG), *tangle*, citada por Divya e Nagaveni (2015) como uma evolução do conceito de blockchain, mas ainda um *ledger* distribuído.

3 ASPECTOS DE PRIVACIDADE E SEGURANÇA EM IOT

Segurança e privacidade são dois conceitos chaves, de fundamental importância no contexto de Internet das Coisas. Ambos são diversas vezes utilizados de forma indiscriminada, como sinônimos, no entanto, são termos com significados distintos. Apesar de possuírem uma relação complexa de interdependência, segurança está relacionada à manutenção dos atributos da informação: confidencialidade, integridade e disponibilidade. Já a privacidade é um conceito relativo, relacionado ao íntimo do indivíduo.

Enquanto a privacidade depende do cumprimento de aspectos técnicos de segurança, ou seja, dependência em um sentido, ela também é citada como um dos princípios de segurança, necessária para estabelecer políticas e regras que definirão aspectos relevantes do sistema. De acordo com Lin *et al.* (2017), a privacidade pode garantir que: (a) os dados só podem ser controlados pelo usuário correspondente; (b) nenhum outro usuário possa acessar o processar os dados; (c) o usuário só possa ter controles específicos baseados nos dados recebidos; (d) o usuário não possa inferir outra informação a partir dos dados recebidos.

3.1 PRIVACIDADE E RISCOS

A privacidade remete a vários conceitos, entre eles o de íntimo, de reserva fora do âmbito social, de preservação do conhecimento alheio, de proteção do indivíduo contra injúrias. No âmbito jurídico, está relacionada ao direito de estar só e de ser deixado só (HIRATA, 2017). A tutela da privacidade foi por longos períodos um tema secundário, até mesmo desmerecido (DONEDA, 2006), iniciando sua relevância apenas no final do século XIX, com o famoso artigo de Warren e Brandeis (1890) “The right to privacy”.

Outras definições foram trazidas por autores, tais como Shils (1966), que relaciona privacidade com interação, comunicação e percepção, onde há um "relacionamento-zero". Já Gavison (1980) sugere que o conceito pode ser estabelecido em termos de quantitativos relacionados a aspectos acerca de alguém (informação, atenção e acesso físico) e identifica 3 componentes da privacidade: o

sigilo, o anonimato e o isolamento ou solidão. Segundo Gavison (1980), esses três elementos são independentes, mas inter-relacionados.

Diversos autores diferenciam intimidade e privacidade. Segundo René Ariel Dotti (1980), intimidade está inserida na vida privada, sendo que os dois conceitos seriam definidos como 2 círculos, o menor sendo a representação da intimidade - teoria dos círculos concêntricos. Considerando a proposta desse autor, intimidade seria mais interno, enquanto que a vida privada englobaria o outro. A intimidade é regida pelo princípio da exclusividade, sendo que este último possui 3 atributos: solidão, que se refere ao desejo de estar só; segredo, que se refere à exigência de sigilo; autonomia, que se refere à liberdade de decidir sobre si mesmo como centro emanador de informações (MARQUES, 2010).

E ainda, baseada na doutrina alemã, tem-se a teoria das esferas (*Sphärentheorie*), citada por diversos estudiosos, incluindo Robert Alexy em sua obra "Teoria dos Direitos Fundamentais" (ALEXY, 2008). Segundo a teoria alemã, é possível separar 3 esferas com graus distintos de proteção: a esfera do segredo, que é a mais interna relacionada a segredos e assuntos extremamente reservados; a esfera íntima, uma intermediária que inclui assuntos de pessoas de confiança; a esfera privada, associada a temas que não se enquadram nas esferas anteriores, mas que se deseja excluir do conhecimento de terceiros (VIEIRA, 2007).

Outros autores ainda expõem ideias semelhantes, com mais níveis de proteção ou esferas com outras nomenclaturas, tais como esfera mais interna, esfera da vida privada e esferas sociais e públicas (SAMPAIO, 1998). No entrando, apesar das nomenclaturas distintas, os termos possuem o mesmo propósito, distinguindo-se basicamente em suas amplitudes (MORAIS, 2002).

Neste caso, ambos serão utilizados como sinônimos neste trabalho, ou seja, a referência ao "direito à privacidade" inclui o à intimidade, à honra, à imagem, à inviolabilidade de domicílio, do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas. Essa uniformização de terminologia também é realizada por alguns trabalhos, quando a padronização dos termos não interfere na análise do tema em questão.

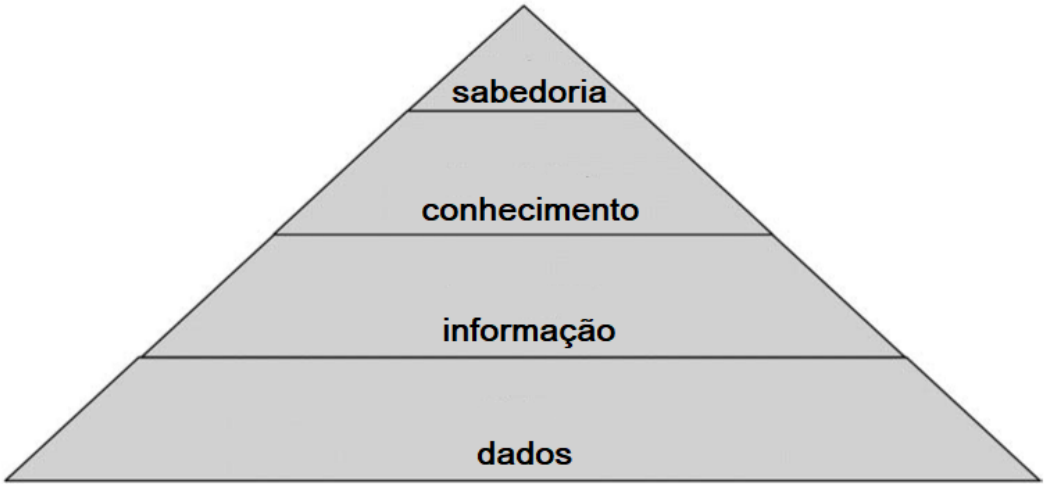
A análise do conceito de privacidade apresentado até o presente momento foi de âmbito geral, sem considerar o *framework* tecnológico existente. Considerando somente o contexto humano, já existe grande complexidade perante a ótica dos direitos individuais; ao acrescentar esta camada ao contexto, as preocupações são

ainda maiores. Se nos primórdios da adoção de tecnologias mais simples, como a fotografia instantânea e jornalismo impresso, houve o surgimento de tamanha preocupação da sociedade com o fim da vida privada, atualmente chegou-se a um cenário antes inimaginável.

No contexto da Internet e Tecnologias da Informação e Comunicação (TICs), o conceito de privacidade está relacionado ao controle sobre a coleção de dados pessoais existentes e quem possui acesso a esse conjunto de informações. De acordo com Mekovec e Vrcek (2011), a preocupação sobre privacidade online envolve: (a) o tipo e a qualidade das informações coletadas; (b) o controle que possuem sobre essas informações e (c) a ciência sobre as práticas de privacidade. Dessa forma, faz-se necessário prover uma forma de controle para o titular dos dados e regular o registro e uso desses dados por terceiros (LIN *et al.*, 2017).

Como pode-se notar, privacidade está intrinsicamente relacionada à informação. De acordo com a pirâmide do conhecimento ou hierarquia DIKW (ELIOT,1934), conforme exibida na Figura 6, os dados são a representação das propriedades dos objetos em sua forma bruta (ACKOFF, 1989), constituindo a base da pirâmide, e, após seu processamento, são transformados em informação. Por esse motivo, a proteção dos dados é um tópico recorrente, que possui um papel fundamental no tema privacidade e segurança dos sistemas computacionais.

Figura 6 – Pirâmide do conhecimento ou hierarquia DIKW



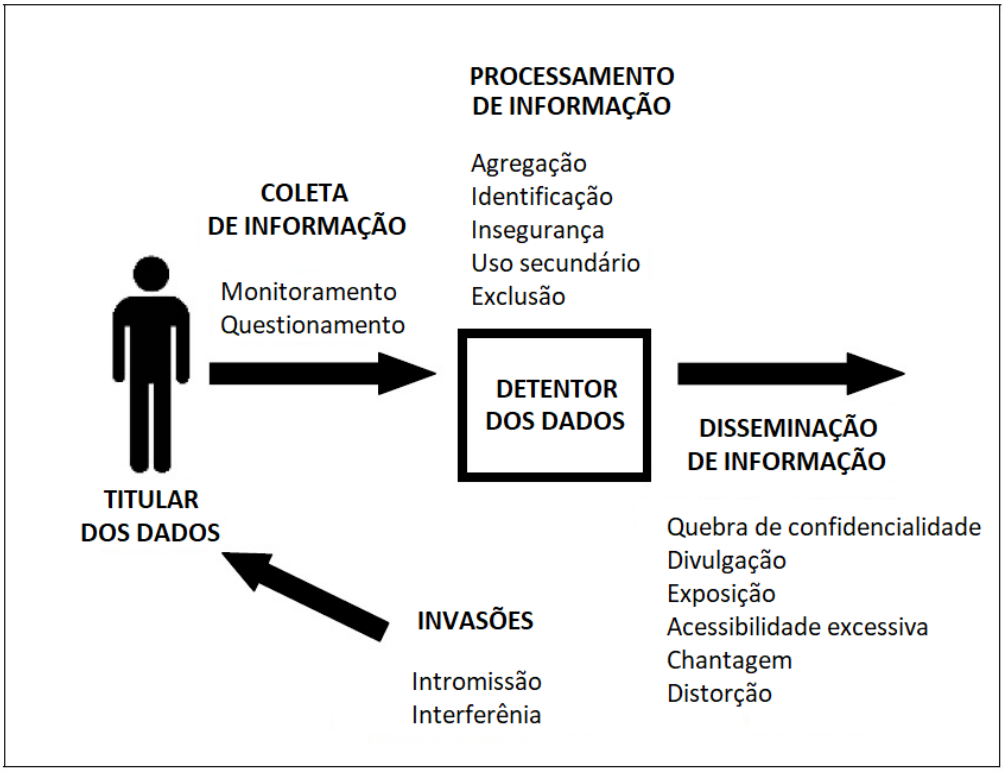
Fonte: Adaptado (traduzido) de Rowley (2007).

Com a evolução das tecnologias de comunicação de dados, o volume de dados coletado, processado, manipulado e transferido alcançou escalas sem precedentes. Devido à aplicação da computação pervasiva e à transparência nas

formas de interação com esses sistemas, esses dados são coletados de forma inconsciente por parte de seus titulares e, muitas vezes, não consentida, o que acarreta diversas consequências.

Solove (2008) propõe uma taxonomia da privacidade, baseada em quatro grupos de atividades que podem criar problemas de privacidade: (a) coleta de informação, (b) processamento de informação, (c) disseminação de informação e (d) invasão. Conforme pode ser observado na Figura 7, essas atividades estão relacionadas com dois atores: (1) o titular de dados, que é o indivíduo diretamente afetado pelas atividades da taxonomia, e (2) o detentor dos dados, que representa as entidades (outras pessoas, empresas, governos) que coletam e processam esses dados.

Figura 7 – Taxonomia da privacidade



Fonte: Adaptado (traduzido) de Solove (2008).

O primeiro grupo de atividades (coleta de informações) está relacionado à captura de dados. A coleta pode ser feita de duas formas: (1) monitoramento e (2) Questionamento. O monitoramento envolve a observação, escuta e gravação das atividades do indivíduo. Por sua vez, o questionamento baseia-se na obtenção da informação através de forma direta, com perguntas ao indivíduo.

O segundo grupo de atividades (processamento de informações) envolve o uso, armazenamento e manipulação dos dados que foram coletados, e pode ocorrer de cinco formas distintas: (1) agregação, que é a combinação de dados de várias fontes acerca de uma pessoa; (2) identificação, que consiste em conectar informações sobre um determinado indivíduo; (3) insegurança, que é o descuido na proteção de informações armazenadas; (4) uso secundário, que é o uso de informação coletada para um propósito diferente do qual o titular consentiu; e (5) exclusão, que é a falha em permitir que o titular saiba que dados os outros têm sobre ele.

O terceiro grupo de atividades (disseminação de informações) refere-se à revelação de dados pessoais ou simplesmente a ameaça de disseminação dessas informações. Isso pode ocorrer de sete formas distintas: (1) quebra de confidencialidade; (2) divulgação; (3) exposição; (4) acessibilidade excessiva; (5) chantagem; (6) apropriação; (7) distorção.

A quebra de confidencialidade, como o próprio nome transmite, é a quebra da promessa de confidencialidade das informações do titular; a divulgação é a revelação de informação confiável que impacta na forma de julgamento dos demais sobre seu caráter, ou seja, na imagem do indivíduo; a exposição envolve expor o corpo, quanto à nudez ou outras funções corporais, ou ainda, a tristeza ou sofrimento do indivíduo.

A acessibilidade excessiva é definida como o aumento do acesso às informações de um indivíduo; a chantagem consiste na ameaça de divulgação de informação pessoal; a apropriação é o uso da identidade do titular em benefício do interesse de terceiro; e a distorção é a disseminação de informação falsa acerca do indivíduo.

Por fim, o quarto grupo de atividades (invasão) refere-se à invasão de assuntos particulares referente ao titular dos dados. A invasão pode ocorrer de duas formas: (1) intromissão, que é perturbar a tranquilidade e isolamento de alguém; (2) interferência, que é a incursão do governo nas decisões do indivíduo sobre seus assuntos privados.

Ponciano *et al.* (2017) discutem privacidade no contexto de Internet das Coisas e elencam, após pesquisa realizada com usuários e vasta análise no tema, um conjunto de três principais preocupações quanto à privacidade dos usuários em

sistemas típicos de IoT: (a) coleta de dados, (b) inferência de informação a partir dos dados coletados e (c) compartilhamento de informação dos usuários com terceiros.

A coleta de dados referenciada neste trabalho segue modelo semelhante ao descrito na taxonomia da privacidade de Solove (2008), citada anteriormente, pois baseia-se na coleta indireta, através dos dispositivos dos usuários, e da coleta direta, através do questionamento. A inferência é a descoberta de novas informações através dos dados coletados dos usuários, que pode ocorrer para diversos propósitos, tais como identificar amigos de usuários e propaganda (e.g. recomendar produtos e serviços). Por fim, o compartilhamento de informações dos usuários com terceiros pode ocorrer como parte de operação do sistema ou devido a uma falha.

Rosner (2016) expõe em seu livro “Privacy and the Internet of Things” 6 riscos à privacidade considerando o contexto de Internet das Coisas: (a) monitoramento intenso, (b) coleta de dados não consentida, (c) coleta de informações médicas, (d) quebras de contexto da informação, (e) diversificação dos stakeholders e (f) vigilância governamental. Esses riscos são listados no Quadro 3.

Vale a pena citar alguns pontos relacionados aos riscos elencados. Relacionado ao risco do "monitoramento intenso" está o direito de privacidade no âmbito do "direito de estar sozinho". Quanto ao risco “coleta de dados não consentida” pode-se discutir também a questão dos dados de crianças e adolescentes, o que aumenta o grau de severidade deste ponto.

Quanto ao risco “coleta deinformações médicas”, o cenário de aplicação é sensores de baixo custo (e.g. em um relógio ou celular) que capturam dados relacionados à saúde da pessoa, juntamente com a aplicação de técnicas de mineração de dados geram informações confiáveis sobre a saúde do indivíduo. Com isso, os consumidores enfrentam diversos riscos e uma situação de vulnerabilidade a constrangimentos e danos à reputação e à discriminação.

Quadro 3 – Riscos à privacidade

Risco	Descrição
1. Monitoramento intenso	Aplicação intensa do sensoriamento, dispositivos conectados para monitoramento da atividade humana. Rastreamento de todos os movimentos das pessoas.
2. Coleta de dados não consentida	Dados de qualquer natureza são coletados, devem haver autorização do titular dos dados, utilização para fins comerciais.
3. Coleta de informações médicas	Dados de dispositivos comuns (e.g. batimentos cardíacos, padrões de soo, pressão sanguínea) se distinguem de informações médicas? Não deveriam estar submetidos à mesma regulamentação? Informações médicas são dados sensíveis que, se divulgadas, colocam os consumidores em posição de vulnerabilidade à constrangimento e danos.
4. Quebra de contextos da informação	Risco gerado pela “fusão de sensores”. Dados de diferentes contextos são reunidos e geram novas informações acerca do indivíduo. Desrespeito do limite das informações de cada contexto é uma violação à privacidade.
5. Diversificação dos *stakeholders*	Elevado volume de dados sendo gerenciado por atores com pouca ou nenhuma experiência sobre políticas de segurança e privacidade.
6. Vigilância governamental	Possível transferência dos dados coletados por empresas privadas para o governo, através de requisição legal.

Fonte: Autoria própria, baseada no livro de Rosner (2016).

Para complementar os riscos e desafios, Tzafestas (2018) traz uma lista de características da Internet das Coisas que podem causar problemas éticos. Essa lista é representada na Tabela 3, com as características e suas respectivas descrições.

As três características citadas no trabalho de Witkowski (2017) (contexto, onipresença e otimização) trazem uma preocupação adicional com questões de segurança e privacidade em IoT. Devido à onipresença, torna-se difícil visualizar os limites entre os espaços públicos e privados, e, somado a isso, com a característica do contexto, pode haver uma sobreposição de informações de diversos cenários da vida dos indivíduos.

E ainda, a otimização pode trazer riscos, dependendo da reação dada pelo objeto e considerando a concessão ou não de permissões do indivíduo afetado pelas consequências da ação tomada pelo objeto, além dos limites e forma do consentimento dado por esse usuário.

Tabela 3 – Características de IoT que podem causar problemas éticos

Característica	Descrição do problema
Miniaturização / Invisibilidade	Dispositivos cada vez menores e transparentes ao usuário, dificultando quaisquer inspeções, auditorias e controle de qualidade
Onipresença / Ubiquidade	Dispositivos em todos os lugares, limites invisíveis entre os espaços públicos e privados, não se sabe o limite da informação
Ultra conectividade	Transferência de alta quantidade de dados (Big Data) que pode ser usada de forma maliciosa
Inteligência incorporada	Objetos inteligentes, dinâmicos e com comportamento emergente, substitutos de uma vida social. A privação desses objetos pode trazer problemas
Comportamento autônomo	Os objetos podem interferir de forma autônoma e espontânea nas atividades humanas, de formas não esperadas pelos usuários e projetistas
Operação descentralizada	Alto fluxo de informação e transferência de dados, dificilmente controlado. Faz-se necessário monitoramento e gerenciamento de modo adequado
Identificação	Objetos possuem uma identidade para se conectarem à rede. O acesso a esses objetos e o gerenciamento dessas identidades pode causar problemas cruciais de segurança e controle
Ambiguidade	A distinção entre objetos naturais, artefatos e humanos será cada vez mais difícil

Fonte: Adaptado de Tzafestas (2018).

3.2 DEFESA DO DIREITO À PRIVACIDADE

No histórico de evolução da sociedade moderna, um dos grandes destaques foi a conquista dos direitos e garantias individuais. Esses direitos fazem parte dos direitos fundamentais (OLIVEIRA; DURÃES, 2014), inerentes à pessoa humana, e estabelecem uma relação de proteção dos indivíduos perante à coletividade, nas relações com todos os seus congêneres. Dentre esses direitos individuais, um está relacionado ao surgimento dessas novas tecnologias e aos conceitos de segurança da informação supracitados, devendo ser assegurado: a privacidade.

O direito à privacidade é uma tipificação dos chamados direitos de personalidade, inatos à personalidade humana (MIRANDA, 1971). Atualmente, a privacidade é considerada um requisito para as liberdades do cidadão, constituindo um dos pilares para a dignidade da pessoa humana, que por sua vez, é um dos fundamentos do Estado Democrático de Direito (SANTANA, 2010).

A própria Constituição Federal (CF) de 1988 prevê em seu artigo 5º, inciso X, que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua

violação” (BRASIL, 1988). Esse importante dispositivo é a principal referência tratando-se desse contexto e possui diversos reflexos, visto que a CF é a base de todo o ordenamento jurídico brasileiro.

Dentro do arcabouço jurídico brasileiro, tem-se diversas legislações que abordam esse tema. Dentre elas, podem-se citar, além da Constituição Federal de 1988, na esfera infraconstitucional, as leis de nº 10.406/2002 (Código Civil), 12.527/2011 (Lei de Acesso à Informação), 12.965/2014 (Marco Civil da Internet), e 13.709/2018, com as alterações promovidas pela Lei 13.853/2019 (Lei Geral de Proteção de Dados Pessoais) (BRASIL, 2002; BRASIL, 2011; BRASIL, 2014; BRASIL, 2018; BRASIL, 2019).

O Código Civil brasileiro trata em seu capítulo II dos direitos de personalidade, entre eles a privacidade, especialmente em seus artigos 20 e 21, conforme é mostrado nos trechos retirados do texto, a seguir:

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. (Vide ADIN 4815)
>
> Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.
>
> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. (Vide ADIN 4815)

A Lei de Acesso à Informação (LAI) possui um papel de extrema importância para a promoção da transparência na Administração Pública. Advinda principalmente do Art 5º, inciso XXXIII da CF, que assegura o "*direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral*", trata do tema em seu Art. 31, conforme é mostrado no trecho do referido artigo, trazido a seguir na íntegra:

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

III - ao cumprimento de ordem judicial;

IV - à defesa de direitos humanos; ou

V - à proteção do interesse público e geral preponderante.

§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

> § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

O Marco Civil da Internet trouxe grande contribuição para os avanços no meio digital além de segurança jurídica relacionada a serviços de tecnologia para a população. A privacidade é abordada em diversos artigos, entre eles, podem ser citados os artigos 8, 10 e 11:

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
>
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
>
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
>
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.
>
> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .
>
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Os artigos 10 a 17 tratam especificamente das obrigações de guarda de registros e dados pessoais. Vale ressaltar, dentre o exposto na legislação, que os registros de conexão devem armazenar somente informações de data e hora de início e término da conexão à Internet, duração e o endereços IP utilizado na comunicação de dados, e não outras informações pessoais, assegurando a privacidade dos usuários.

Essa mesma legislação também foi o trouxe a questão dos dados pessoais. Em seu Art 3º, apresenta os princípios do uso da Internet no Brasil e, dentre eles, está a proteção dos dados pessoais. O Art 7º também possui diversos incisos relacionados com a privacidade, tais como I, II e III, conforme a seguir (in verbis):

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;.

E ainda, apresenta regras quanto aos dados pessoais que serviram como base para legislações posteriores, como será visto a seguir:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

Essas legislações traziam em seus dispositivos referências ao tratamento de dados pessoais, porém não eram voltadas para tal. A Lei Geral de Proteção de Dados Pessoais (LGPD) surge como uma importante normativa acerca do tema, que objetiva proteger os direitos de liberdade e de privacidade da pessoa natural, além do livre desenvolvimento da sua personalidade. De acordo com a lei, em seu Art. 5º, inciso X, tratamento é definido como:

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

A privacidade aparece em seu Art 2º, inciso I, o qual apresenta o respeito à privacidade como um dos fundamentos da proteção de dados pessoais. A Lei também traz a definição de alguns conceitos importantes, ilustrados no Quadro 4.

Quadro 4 – Definições sobre dados de acordo com a LGPD

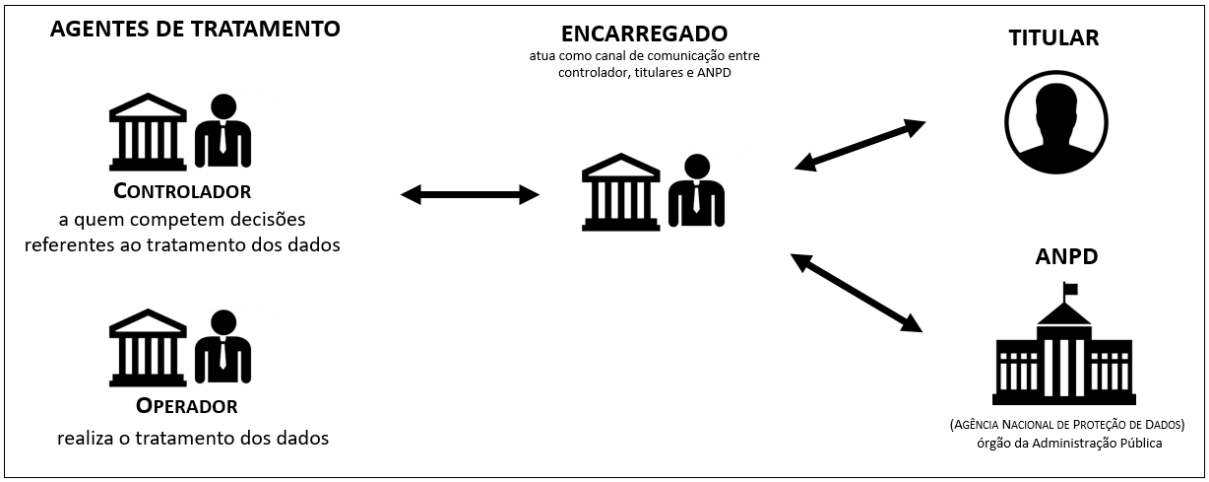
Conceito	Descrição
1. Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável
2. Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
3. Dado anonimizado	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento

Fonte: Autoria própria, baseada na redação da LGPD.

Além disso, apresenta alguns atores neste cenário, que são: (a) o titular dos dados, definida como “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”; (b) agentes de tratamento, que podem ser a figura do controlador ou do operador, ambos sendo pessoas natural ou jurídica, de direito público ou privado; (c) encarregado, que pela lei é “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)” e (d) ANPD, definida como “órgão da administração pública responsável por zelar, implementar e

fiscalizar o cumprimento desta Lei em todo o território nacional". O relacionamento desses envolvidos é ilustrado na Figura 8.

Figura 8 – Relacionamento entre os envolvidos de acordo com a LGPD



Fonte: Autoria própria.

A LGPD ainda estabelece um conjunto de princípios em seu Art. 6º, conforme pode ser verificado no Quadro 5. E ainda, esses princípios devem observar a boa-fé.

O tratamento de dados pessoais ao qual a lei se refere é inclusive nos meios digitais (mas não somente), independente do meio, do país da sede e do país onde estejam localizados os dados, desde que (a) o tratamento (a.1) seja realizado em território nacional ou (a.2) tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou (b) a coleta de dados seja realizada em território nacional. Vale ressaltar que está fora do âmbito de aplicação desta lei os casos previstos no Art 4º.

Outros dispositivos jurídicos também estão relacionados com a privacidade, dentre os quais podem-se citar o *habeas data*, remédio constitucional que possui rito processual disciplinado na lei nº 9.507/1997, a lei nº 9.472/1997 (Lei Geral de Telecomunicações), que trata em seu Art. 3º da inviolabilidade e ao segredo da comunicação, a lei nº 8.078/1990 (Código de Defesa do Consumidor), que trata em seu Art. 43 das informações e dados pessoais em bancos de dados e cadastros de consumidores, e ainda, a lei nº 2.414/2011 (Lei do Cadastro Positivo), que disciplina através de seus diversos artigos a formação e a consulta a bancos de dados com informações de adimplemento de pessoas naturais e jurídicas (BRASIL, 1990; BRASIL, 1997a; BRASIL, 1997b). No caso, as informações de pessoas naturais seriam o foco dessa observação.

Quadro 5 – Princípios para as atividades de tratamento de dados pessoais da LGPD

Princípios	Descrição
1. Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
2. Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
3. Necessidade	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
4. Livre acesso	Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
5. Qualidade dos dados	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
6. Transparência	Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
7. Segurança	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
8. Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
9. Não discriminação	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
10. Responsabilização e prestação de contas	Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Fonte: Autoria própria, de acordo com redação da LGPD, Art 6º.

Para verificação de artigos específicos da legislação brasileira relacionados à privacidade e dados pessoais podem ser consultados no trabalho de Costa (2019), que apresenta em seu trabalho acadêmico proposta semelhante à realizada neste capítulo, porém dispõe uma elicitação simplificada em formato de tabela.

Vale ressaltar que o Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet, possui alguns dispositivos de grande importância ao tema, contidos na Seção II, intitulada “Padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas” (BRASIL, 2016). O Art. 13, especificamente, trata da segurança, trazendo um conjunto de diretrizes sobre padrões de segurança que devem ser observados pelos provedores de conexão e de aplicações.

3.3 SOLUÇÕES

Segurança e privacidade no contexto da Internet das Coisas trazem diversos desafios, como destacado no decorrer deste trabalho. Porém, blockchain surge como uma tecnologia promissora a fim de resolver problemas enfrentados neste cenário.

Por ser uma rede *peer-to-peer* distribuída e promover a camada de segurança de forma transparente, sem necessidade de um entidade centralizadora, surge como idealmente utilizada nesse cenário para prover privacidade e segurança. Diversos trabalhos foram propostos para esta finalidade e, em geral, propõem blockchains modificadas.

Alguns trabalhos que focam no uso de blockchain para autenticação e controle de acesso. Novo (2018) propõe a utilização de uma blockchain pública sem permissionamento com hubs de gerenciamento e a utilização de contratos inteligentes para definição do controle de acesso. Abordagem semelhante é proposta por Rifi *et al.* (2017), porém, que utiliza múltiplos contratos inteligentes ao invés de um único. Já Alphand *et al.* (2018) propõem a utilização de uma blockchain pública não permissionada com servidores de recursos e utilização de contratos inteligentes, criados pelos donos dos recursos contendo as permissões de acesso e publicados na rede.

Outra proposta é trazida por Dorri *et al*. (2017), que propõem *Lightweight Scalable BC* (LSB), uma blockchain otimizada para IoT para prover segurança e privacidade. Nesse blockchain, os autores desenvolveram um algoritmo de consenso que elimina a necessidade de resolução de problemas matemáticos, porém incorpora um método de confiança distribuído em que o tempo de validação de novos blocos reduz conforme há novas validações.

A proposta trazida pelos pesquisadores brasileiros Pinno, Gregio e Bona (2017) é uma blockchain denominada ControlChain, que provê uma arquitetura transparente ao usuário, totalmente descentralizada, escalável e tolerante a falhas. Ela baseia-se no uso de quatro blockchains, na qual três delas são para consulta a fim de tomadas de decisão acerca do controle de acesso e a última é usada para armazenamento dessas decisões.

E ainda, Hammi *et al.* (2018) apresentam um mecanismo de autenticação baseado em blockchain denominado *Bubbles of Trust*, criado sobre a blockchain

pública Ethereum, que visa a criação de zonas virtuais seguras onde os dispositivos podem se comunicar. Além disso, fizeram um estudo acerca do impacto de energia e financeiro, visto que um dos maiores problemas com o uso de blockchain é o consumo de energia, o que torna um desafio no cenário de recursos de energia limitados como IoT.

Os dois maiores desafios para blockchain no contexto de IoT são: (a) alto processamento e (b) armazenamento. Como pôde ser visto na definição e características dessa tecnologia, o armazenamento de toda a base de dados em cada nó tornaria o uso em Internet das Coisas, que já possuem recursos limitados, inviável. O alto processamento exigido para a resolução de problemas criptográficos pelos mineradores também trazem o desafio para o seu uso, além do consumo de energia.

Visto que os limites da privacidade para cada usuário são distintos e dependem de características pessoais do indivíduo, não há um algoritmo ou única solução para resolução da questão da privacidade. Ponciano *et al.* (2017) propõem um conjunto de heurísticas para lidar com os desafios e preocupações que a privacidade impõe no contexto de Internet das Coisas, listado no Quadro 6.

Quadro 6 – Heurísticas para privacidade em IoT

Heurística	Descrição
1. Deixe o usuário ciente sobre que informações pessoais o sistema retém	Os usuários podem não entender o processo de coleta de dados, tendo em vista que em IoT os dados podem ser coletados indiretamente (coleta ubíqua). Uma forma de atender essa heurística é permitir que o usuário acesse ou realize o download dos dados coletados e inferidos.
2. Deixe claro o propósito dos dados para cada recurso	Os usuários tendem a sentir-se menos preocupados com privacidade quando entendem o uso dos dados por um determinado recurso.
3. Deixe a troca de dados com terceiros explícita e configurável	A troca de dados pessoais com terceiros é uma das maiores preocupações dos usuários quanto à privacidade. Isso não pode ser feito sem o conhecimento e autorização explícita do usuário, portanto, não pode ser uma configuração padrão do sistema. O sistema deve fornecer ao usuário a possibilidade de especificar que dados serão fornecidos ou não.
4. Realize avaliações empíricas de privacidade	Resultados de pesquisas mostram que diversas questões de privacidade não podem ser generalizadas, variam de acordo com o sistema. Novos sistemas podem fornecer recursos que promovam riscos significativos à privacidade dos usuários. Os efeitos de tais funcionalidades devem ser testados antes do sistema ser disponibilizado.

Fonte: Adaptado de Ponciano *et al.* (2017).

Rosner (2016) ainda sugere a aplicação de algumas táticas a fim de aumentar a privacidade, dentre elas estão a minimização de dados, aplicação de técnicas de anonimização de dados e a utilização de frameworks. Vários autores sugerem a aplicação de técnicas de anonimização de dados ao lidar com dados sensíveis a fim de preservar a privacidade, tal como Brito e Machado (2017) independente de uso ou não de blockchain.

3.4 QUESTÕES EM ABERTO

Como pode ser observado a partir das seções anteriores, a Internet das Coisas apresenta um cenário bastante complexo de desenvolvimento e implantação. Porém essa infraestrutura global de objetos distribuídos e interconectados tem um enorme potencial que deve ser explorado.

Blockchain surge como uma tecnologia estado da arte para resolver questões relacionadas a características intrínsecas de IoT, portanto, fazendo uma análise do contexto, a junção de ambas as áreas desponta como uma excelente alternativa. No entanto, existem alguns aspectos que necessitam ser considerados, dentre eles, a compatibilidade da tecnologia com pontos específicos da LGPD, tais como: (a) a exclusão e (b) o papel do controlador dos dados.

A Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais, trata em seu Art. 16 a questão da exclusão dos dados (in verbis) (BRASIL, 2018):

> O Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Como foi visto em seções anteriores, blockchain conceitua-se como uma estrutura de rede P2P e livro-razão de registros imutáveis. Portanto, o conceito básico de funcionamento de blockchain baseia-se na imutabilidade e na descentralização.

Uma vez que uma informação seja adicionada à cadeia de blocos, não poderá ser modificada ou alterada. O participante que entra na rede terá uma cópia desses registros e não poderá excluir dados, apenas adicionar novas informações em blocos seguintes. Com isso, surge um conflito entre a LGPD no que tange à exclusão de dados e a imutabilidade da blockchain.

A exclusão também está ligada ao direito ao esquecimento que, apesar de não regulamentada, possui base na LGPD e é fortalecida com julgados (GALLI, 2018) e outros dispositivos legais. O direito ao esquecimento seria proveniente do direito à privacidade e fundamentado no princípio da dignidade da pessoa humana, assegurando que fatos que causem constrangimento não sejam armazenados e disponibilizados.

Esse direito é citado no enunciado 531 da VI Jornada de Direito Civil do CJF/STJ como uma expressão da dignidade da pessoa humana e é baseado no Art. 11 do Código Civil, conforme citação a seguir: "*A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento*" (CJF, 2013). Contudo, no próprio cenário jurídico, há conflitos entre os limites da liberdade de expressão e do acesso à informação com os do direito ao esquecimento.

Vale ressaltar que, em geral, as informações contidas em uma blockchain são dados de transações anônimas, porém há a possibilidade de inserção de informações pessoais na cadeia de blocos, conhecido pelo termo "envenenamento por privacidade" ou "*blockchain privacy poisoning*" (LINDSEY, 2019), que gera o conflito referenciado anteriormente.

E ainda, a LGPD atribui responsabilidades aos controladores de dados. Porém, nenhum participante da rede pode ser definido com este papel em uma rede blockchain pública; devido à descentralização, não há este papel.

Além do uso de blockchain, também foram propostas soluções com aplicações de diretrizes, heurísticas e análises acerca da segurança e privacidade, que envolvem o conceito de "*Privacy-by-Design*". Porém, as dificuldades técnicas inerentes ao contexto para implementação das soluções IoT tornam difícil a adoção

dessas práticas, principalmente desde o início do projeto. Em geral, esses requisitos acabam sendo deixados para melhorias pós-implantação.

Com o amadurecimento da área e com a popularização dos conceitos relacionados a esses problemas, novos debates, alternativas e soluções surgirão para diminuir a lacuna desses conflitos.

4 CONCLUSÃO

A Internet das Coisas revolucionou o cenário mundial, agregando áreas, ideias e tecnologias já existentes em um único conceito. Redes de Sensores Sem Fio, RFID, IPv6, Internet, diferentes protocolos de comunicação, aplicações *web*, indústria 4.0, Big Data, mineração de dados, computação em nuvem, entre outros termos, estão associados a essa infraestrutura de rede global que promete ligar todas as coisas.

A inovação advinda desse universo ultrapassou as previsões de ubiquidade existentes, trazendo novos temas e impactos tecnológicos e sociais que necessitam ser discutidos. A tecnologia de forma transparente envolve interação entre pessoas, entre pessoas e objetos e entre as próprias coisas. Porém, mesmo na interação entre artefatos computacionais, é necessário analisar os conceitos humanos envolvidos, que podem trazer riscos aos usuários.

A segurança e a privacidade emergem como requisitos essenciais neste campo de aplicações. Porém, mesmo havendo a necessidade de atendimento a esses requisitos, ainda há muitos desafios no próprio desenvolvimento de aplicações IoT para serem superados, e ainda, lacunas trazidas pela própria aplicação dos requisitos de segurança e privacidade nesse contexto.

Este trabalho apresentou uma visão geral de segurança e privacidade em Internet das Coisas, apresentando a área, alguns desafios e como algumas soluções buscam transpor esses problemas, como com o uso de blockchain. Blockchain surge como um novo paradigma, com conceitos que vão ao encontro dos principais problemas enfrentados por Internet das Coisas. Porém, ainda assim, a sua aplicação traz questões, principalmente quando tratamos de dados pessoais.

O trabalho apresentou como essas questões estão relacionadas a legislações, apresentando brevemente o arcabouço jurídico brasileiro correlato ao tema em questão. Além disso, a pesquisa mostrou visões do contexto humano e tecnológico, assim como uma análise das questões em aberto e de conflito existentes.

Com a difusão dos dados pessoais e a pervasividade trazida pela adoção dessas tecnologias em Internet das Coisas, torna-se fundamental a reflexão acerca da segurança e privacidade desde o projeto das novas soluções, a aplicação de

medidas para assegurar o direito dos usuários e da esfera privada. Trabalhos futuros envolvendo cada um desses temas trarão diversos benefícios para a sociedade e amadurecimento da área.

REFERÊNCIAS

ABAD, E. *et al*. **RFID smart tag for traceability and cold chain monitoring of foods**: Demonstration in an intercontinental fresh fish logistic chain. Journal of food engineering, v. 93, n. 4, 2009. p. 394-399.

ACKOFF, R. L. **From data to wisdom**. Journal of applied systems analysis, v. 16, n. 1, 1989. p. 3-9.

ALAA, M. *et al*. A review of smart home applications based on Internet of Things. **Journal of network and computer applications**, v. 97, 2017. p. 48-65.

ALBUQUERQUE, R. O. **Uma proposta de um modelo de confiança computacional para grupos em sistemas distribuídos**. 2008. Tese (Doutorado em Engenharia Elétrica) – Faculdade de Tecnologia, Universidade de Brasília, 2008.

ALEXY, R. **Teoria dos direitos fundamentais**. 2008.

ALPHAND, O. *et al*. **IoTChain**: A blockchain security architecture for the Internet of things. In: 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2018. p. 1-6.

ASHTON, K. **That 'Internet of Things' thing**. RFID journal, v. 22, n. 7, 2009. p. 97-114.

ATZORI, L.; IERA, A.; MORABITO, G. **The Internet of Things**: A survey. **Computer networks**, v. 54, n. 15, 2010. p. 2787-2805.

BANAFA, A. **IoT and blockchain convergence**: benefits and challenges. IEEE Internet of things, 2017.

BANERJEE, M.; LEE, J.; CHOO, K. K. R. **A blockchain future for internet of things security: a position paper**. Digital communications and networks, v. 4, n. 3, 2018. p. 149-160.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 fev. 2020.

BRASIL. **Lei n. 8.078/1990, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 10 fev. 2020.

BRASIL. **Lei n. 9.472, de 16 de julho de 1997**. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. 1997a. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9472.htm>. Acesso em: 10 fev. 2020.

BRASIL. **Lei n. 9.507/1997, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. 1997b. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm>. Acesso em: 10 fev. 2020.

BRASIL. **Lei n. 10.406/2002, de 10 de janeiro de 2002**. Institui o Código Civil. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 10 fev. 2020.

BRASIL. **Lei n. 12.527/2011, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 10 fev. 2020.

BRASIL. **Lei n. 12.965/2014, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 fev. 2020.

BRASIL. **Decreto nº 8.771/2016, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 10 fev. 2020.

BRASIL. **Lei n. 13.709/2018, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10 fev. 2020.

BRASIL. **Lei n. 13.853/2019, de 08 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm>. Acesso em: 10 fev. 2020.

BRITO, F. T.; MACHADO, J. C. **Preservação de privacidade de dados**: Fundamentos, técnicas e aplicações. Jornadas de atualização em informática, 2017.

CHIANG, M.; ZHANG, T. **Fog and IoT: An overview of research opportunities**. IEEE Internet of things journal, v. 3, n. 6, 2016. p. 854-864.

CHICARINO, V. R. *et al*. Uso de blockchain para privacidade e segurança em internet das coisas. In: Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Brasília: SBC, p. 28, 2017.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. **IEEE Access**, v. 4, 2016. p. 2292-2303.

CISCO. **Internet of Things**. Cisco. 2016. Disponível em: <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf>. Acesso em: 30 jan. 2020.

CJF (Conselho de Justiça Federal). VI Jornada de direito civil. Brasília, 2013. Disponível em: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/vijornadadireitocivil2013-web.pdf>. Acesso em: 31 jan. 2020.

CONDOLUCI, M. *et al*. **5g IoT industry verticals and network requirements**. In: Powering the Internet of Things With 5G Networks. IGI Global, 2018. p. 148-175.

CONOSCENTI, M.; VETRO, A.; MARTIN, J. C. de. **Blockchain for the Internet of things**: A systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). IEEE, 2016. p. 1-6.

CONTI, M. *et al*. **Internet of things security and forensics**: Challenges and opportunities. Elsevier, 2018.

COSTA, M. F. N. **Internet das coisas**: a proteção da privacidade em um mundo conectado. 2019. Trabalho de Conclusão de Curso (Especialização em Governança e Controle da Regulação em Infraestrutura), Escola Nacional de Administração Pública, 2019.

DA XU, L.; HE, W.; LI, S. **Internet of Things in industries**: A survey. IEEE Transactions on industrial informatics, v. 10, n. 4, 2014. p. 2233-2243.

DELICATO, F. C. **Middleware baseado em serviços para redes de sensores sem fio**. 2005. Tese (Doutorado) – Programa de Pós-Graduação de Engenharia, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2005.

DIAS, R. P. N. **Análise de plataformas blockchain**. 2019. Dissertação (Mestrado em Engenharia Informática) – Faculdade de Ciências e Tecnologia, Universidade de Coimbra, 2019.

DIVYA, M.; BIRADAR, N. B. IOTA-next generation block chain. **International journal of engineering and computer science**, v. 7, n. 04, 2018. p. 23823-23826.
DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DORRI, A. *et al*. **LSB**: A lightweight scalable blockchain for iot security and privacy. Dezembro de 2017. Disponível em: <https://arxiv.org/pdf/1712.02969.pdf>. Acesso em: 20 jan. 2020.

DORRI, A.; KANHERE, S. S.; JURDAK, R. **Blockchain in Internet of Things**: challenges and solutions. Agosto de 2016. Disponível em: <https://arxiv.org/ftp/arxiv/papers/1608/1608.05187.pdf>. Acesso em: 21 jan. 2020.

DOTTI, R. A. **Proteção da vida privada e liberdade de informação**: possibilidades e limites. Editora Revista dos Tribunais, 1980. São Paulo: RT, 1980.

EJAZ, W. *et al*. **Efficient energy management for the internet of things in smart cities**. IEEE Communications magazine, v. 55, n. 1, 2017. p. 84-91.

ELIOT, T. S. The Rock, chapter Part I. London: Faber & Faber, 1934.

ELKHODR, M.; SHAHRESTANI, S.; CHEUNG, H. **The internet of things: new interoperability, management and security challenges**. International journal of network security & its applications, 2016. p. 85-102.

GALLI, M. **STJ aplica direito ao esquecimento e obriga sites de busca a filtrar resultados**. Consultor Jurídico. Publicado em: 09 mai. 2018. Disponível em: <https://www.conjur.com.br/2018-mai-09/stj-obriga-sites-busca-filtrar-resultados-promotora>. Acesso em: 30 jan. 2020.

GAVISON, R. **Privacy and the limits of law**. The Yale law journal, v. 89, n. 3, 1980. p. 421-471.

GIUSTO, D. *et al*. **The Internet of Things**: 20th Tyrrhenian workshop on digital communications. Springer Science & Business Media, 2010.

GUBBI, J. *et al*. **Internet of Things (IoT)**: A vision, architectural elements, and future directions. Future generation computer systems, v. 29, n. 7, 2013. p. 1645-1660.

HAMMI, M. T. *et al*. **Bubbles of Trust**: A decentralized blockchain-based authentication system for IoT. Computers & security, v. 78, 2018. p. 126-142.

HE, H. *et al*. **The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence**. In: 2016 IEEE Congress on Evolutionary Computation (CEC). IEEE, 2016. p. 1015-1021.

HIRATA, A. **Direito à privacidade**. Enciclopédia jurídica da PUC-SP. 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.

KHAN, M. A.; SALAH, K. **IoT security**: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, v. 82, 2018. p. 395-411.

KIM, Jaewoo *et al*. **M2M service platforms: Survey, issues, and enabling technologies**. IEEE Communications surveys & tutorials, v. 16, n. 1, 2013. p. 61-76.

LIN, J. *et al*. **A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications**. IEEE Internet of things journal, v. 4, n. 5, 2017. p. 1125-1142.

LINDSEY, N. **Blockchain privacy poisoning a new concern in post-GDPR era**. CPO Magazine. Publicado em: 14 mar. 2019. Disponível em: <https://www.cpomagazine.com/data-protection/blockchain-privacy-poisoning-a-new-concern-in-post-gdpr-era/>. Acesso em: 30 jan. 2020.

LIU, C. *et al*. External integrity verification for outsourced big data in cloud and IoT: A big picture. **Future generation computer systems**, v. 49, 2015. p. 58-67.

MACHADO, R. N. **Análise sobre otimização de blockchain para internet das coisas**. 2018. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação), Universidade Federal de Pernambuco, 2018.

MADAKAM, S. *et al*. **Internet of Things (IoT)**: A literature review. Journal of computer and communications, v. 3, n. 5, 2015. p. 164.

MANO, L. Y. *et al*. **Explorando tecnologias de IoT no contexto de Health Smart Home: uma abordagem para detecção de quedas em pessoas idosas**. Journal on advances in theoretical and applied informatics, v. 2, n. 1, 2016. p. 46-57.

MANRIQUE, J. A.; RUEDA-RUEDA, J. S.; PORTOCARRERO, J. M. T. **Contrasting internet of things and wireless sensor network from a conceptual overview**. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2016. p. 252-257.

MARQUES, A. N. G. **Direito à intimidade e privacidade**. Jus vigilantibus, 2010.

MCKINSEY & COMPANY. **Growing opportunities in the Internet of Things**. Copyright© 1996-2020 McKinsey & Company. Julho de 2019. Disponível em: <https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things>. Acesso em: 30 jan. 2020.

MEKOVEC, R.; VRČEK, N. **Factors that influence Internet users' privacy perception**. In: 33rd International Conference on Information Technology Interfaces. Proceedings of the ITI 2011. IEEE, 2011. p. 227-232.

MIRANDA, P. de. **Tratado de direito privado**. Rio de Janeiro: Borsoi, 1971.

MORAIS, A. de. **Direito constitucional**. 12. ed. São Paulo: Atlas, 2002. 80 p.

MOUGAYAR, W. **Blockchain para negócios**: promessa, prática e aplicação da nova tecnologia da internet. Rio de Janeiro: Alta Books Editora, 2018.

NAKAMOTO, S. *et al*. **Bitcoin: A peer-to-peer electronic cash system**. 2008. NIC (National Intelligence Council). Disruptive civil technologies: Six technologies with potential impacts on us interests out to 2025. 2008. Disponível em: <https://fas.org/irp/nic/disruptive.pdf>. Acesso em: 28 jan. 2020.

NOVO, O. **Blockchain meets IoT**: An architecture for scalable access management in IoT. IEEE Internet of things journal, v. 5, n. 2, 2018. p. 1184-1195.

OLIVEIRA, M. K. de; DURÃES, N. S. S. Os direitos fundamentais na sociedade brasileira contemporânea. **Organizações e sociedade**, v. 3, 2014.

PEÑA-LÓPEZ, I. *et al*. **ITU Internet report 2005**: the Internet of Things. 2005. Disponível em: <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>. Acesso em: 27 jan. 2020.

PINNO, O. J. A.; GREGIO, A. R. A.; BONA, L. C. E. de. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In: GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017. p. 1-6.

PONCIANO, L. *et al*. **Designing for Pragmatists and Fundamentalists**: Privacy Concerns and Attitudes on the Internet of Things. In: XVI Brazilian Symposium on Human Factors in Computing Systems. 2017. p. 1-10.

RAJ, P.; RAMAN, A. C. **The Internet of Things**: Enabling technologies, platforms, and use cases. Auerbach Publications, 2017.

RIFI, N. *et al*. **Towards using blockchain technology for IoT data access protection**. In: 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB). IEEE, 2017. p. 1-5.

ROSNER, G. **Privacy and the Internet of Things**. O'Reilly Media, Incorporated, 2016.

ROWLEY, J. **The wisdom hierarchy: representations of the DIKW hierarchy**. Journal of information science, v. 33, n. 2, 2007. p. 163-180.

SAGHIRI, A. M. *et al*. **A framework for cognitive Internet of things based on blockchain**. In: 2018 4th International Conference on Web Research (ICWR). IEEE, 2018. p. 138-143.

SALMAN, T.; JAIN, R. **Networking protocols and standards for internet of things**. Internet of things and data analytics handbook, v. 2015, 2015. p. 215-238.

SAMPAIO, J. A. L. **Direito à intimidade e a vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte**. Del Rey, 1998.

SANG, K. S. *et al*. **Study of Group Route Optimization for IoT Enabled Urban Transportation Network**. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2017. p. 888-893.

SANTANA, R. S. de. **A dignidade da pessoa humana como princípio absoluto**. Direito net, v. 17, 2010.

SATTAROVA F. Y.; KIM, T. H. **IT security review: Privacy, protection, access control, assurance and system security**. International journal of multimedia and ubiquitous engineering, v. 2, n. 2, 2007. p. 17-32.

SETHI, P.; SARANGI, S. R. **Internet of Things**: architectures, protocols, and applications. Journal of electrical and computer engineering, v. 2017, 2017.

SHA, K. *et al*. **On security challenges and open issues in Internet of things**. Future generation computer systems, v. 83, 2018. p. 326-337.

SHILS, E. Privacy: Its constitution and vicissitudes. **Law and contemporary problems**, v. 31, n. 2, p. 281-306, 1966.

SICARI, S. *et al*. **Security, privacy and trust in Internet of Things**: The road ahead. Computer networks, v. 76, 2015. p. 146-164.

SINGH, S.; SINGH, N. **Internet of Things (IoT)**: Security challenges, business opportunities & reference architecture for E-commerce. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE, 2015. p. 1577-1581.

SOLOVE, D. J. **Understanding Privacy**. Harvard University Press. 2008.

SOMMERVILLE, I. **Software engineering**. 9. ed. Pearson, 2011.

THAKUR, T. T. *et al*. **Real time traffic management using Internet of Things**. In: 2016 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2016. p. 1950-1953.

TIAN, F. **A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things**. In: 2017 International conference on service systems and service management. IEEE, 2017. p. 1-6.

TZAFESTAS, S. G. **Ethics and law in the internet of things world**. Smart cities, v. 1, n. 1, 2018. p. 98-120.

VERMESAN, O. *et al*. **Internet of things strategic research roadmap**. Internet of things-global technological and societal trends, v. 1, n. 2011, 2011. p. 9-52.

VIEIRA, T. M. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito, Universidade de Brasília, 2007.

WARREN S.; BRANDEIS, L. **The right to privacy**. Harvard law review, 1890. p. 193-220.

WEF (World Economic Forum). **The global risks report 2020**. Copyright© 2020 World Economic Forum. Disponível em: <https://www.weforum.org/reports/the-global-risks-report-2020>. Acesso em: 01 fev. 2020.

WEISER, M. **The Computer for the 21 st century**. Scientific american, v. 265, n. 3, p. 94-105, 1991.

WITKOWSKI, K. **Internet of things, big data, industry 4.0–innovative solutions in logistics and supply chains management**. **Procedia engineering**, v. 182, 2017. p. 763-769.

YANG, G. *et al*. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. **IEEE Transactions on industrial informatics**, v. 10, n. 4, 2014. p. 2180-2191.

YANG, Y. *et al*. **A survey on security and privacy issues in internet-of-things**. IEEE Internet of things journal, v. 4, n. 5, 2017. p. 1250-1258.

YEH, K. H. **A secure IoT-based healthcare system with body sensor networks**. IEEE Access, v. 4, 2016. p. 10288-10299.

YU, B. *et al*. **Trust chain**: Establishing trust in the iot-based applications ecosystem using blockchain. IEEE Cloud computing, v. 5, n. 4, 2018. p. 12-23.

YU, L.; LU, Y.; ZHU, X. J. Smart hospital based on internet of things. **Journal of networks**, v. 7, n. 10, p. 1654, 2012.

ZANELLA, A. *et al*. **Internet of things for smart cities.** IEEE Internet of things journal, v. 1, n. 1, 2014. p. 22-32.

ZARPELÃO, B. B. *et al*. **A survey of intrusion detection in Internet of things**. Journal of network and computer applications, v. 84, 2017. p. 25-37.

ZHANG, Zhi-Kai *et al*. **IoT security**: ongoing challenges and research opportunities. In: 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, 2014. p. 230-234.