# Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)

**Nairobi Spiecker de Oliveira[1], Moises Alexandre Gomes[2], Ronaldo Lopes[3], Jéferson C. Nobre[4]**

[1]Curso Superior de Tecnologia em Segurança da Informação
Universidade do Vale do Rio dos Sinos (UNISINOS)
São Leopoldo – RS – Brazil

{nspiecker, magomes, rlsanlo, jcnobre}@edu.unisinos.br

***Abstract.*** *In recent years, a remarkable growth of small technological devices connected to the Internet has been identified, exchanging information generating the concept of Internet of Things (IoT). Many of these devices are found supporting various business models. Devices ranging from cardiac sensors (HealthCare) to clocks, microwaves and even earthquake, hurricane and Tsunami sensors are fundamental to modern society. While there are numerous technology concerns regarding the restriction of processing, memory, bandwidth and power due to the reduced size of these devices, little is known about how to achieve the necessary levels of security in order to comply with a set of country legislations for these devices. In this article we will address the information security under aspects of the Brazilian law that deals with the protection of data of users, General Data Protection Law (LGPD), applied to IoT. Aspects such as the collection, transmission and storage of personal and confidential data described in the law are challenges when we talk about restricted devices. This will address the main concepts required by the LGPD as well as the discussion about the applicability of security concepts in these devices in order to comply with the LGPD.*

***Resumo.*** *Nos últimos anos, identificou-se um crescimento notável de pequenos dispositivos tecnológicos conectados à internet trocando informações gerando o conceito de Internet das Coisas (Internet of Things - IoT). Muitos destes dispositivos são encontrados apoiando diversos modelos de negócio. Dispositivos que vão desde sensores cardíacos (HealthCare) passando por relógios, microondas e até sensores de terremotos, furacões e Tsunamis sendo estes fundamentais para a sociedade moderna. Embora existam inúmeras preocupações por parte da tecnologia quanto a restrição de processamento, memoria, bandwidth e energia devido ao tamanho reduzido destes dispositivos, pouco sabe-se sobre como alcançar níveis necessários de segurança afim de cumprir um conjunto de legislações de países para estes dispositivos. No presente artigo iremos abordar a segurança da informação sob os aspectos da lei brasileira que trata da proteção de dados dos usuários, Lei Geral de Proteção de Dados (LGPD), aplicada a IoT. Aspectos como coleta, transmissão e armazenamento de dados pessoais e sigilosos descritos da lei são desafios quando falamos de dispositivos restritos. Desta forma serão abordados os principais conceitos requeridos pela LGPD assim como a discussão sobre a aplicabilidade dos conceitos de segurança nestes dispositivos visando estar em conformidade com a LGPD.*

## 1. Introdução

A internet tem realizado uma verdadeira revolução no cotidiano das pessoas. Boa parte disto ocorre devido ao aumento da conectividade entre os indivíduos proporcionada por ela, seja através dos computadores ou dispositivos inteligentes de computação móvel conhecidos por *smartphones* [Oulasvirta et al. 2012]. Conforme o dados do ultimo censo realizado pelo IBGE, existem hoje cerca de 1,26 telefones celulares para cada habitante [IBGE 2017] Segundo o site [World IPv6 Launch 2018], o alicerce para este crescimento pode ser justificado pela Internet das Coisas (IOT).

Esta revolução tecnológica trouxe consigo importantes inovações e possibilidades relacionadas a área de negócios, pesquisas, nichos de mercado assim como novos desafios [LEMOS and MARQUES 2018]. Segundo [Forbes 2014], além do IPv6 também atribui-se a crescente disponibilidade da Internet através da banda larga e a redução do custo desta, o aumento no desenvolvimento de dispositivos com capacidade restrita e sensores Wi-Fi acoplados.

Neste contexto apareceram tecnologias voltas para IoT, onde a ideia por trás deste conceito teve origem em novas possibilidades originadas através de dispositivos inteligentes conectados a internet, que possibilitassem desta forma, a comunicação a partir de qualquer lugar a qualquer momento por um dispositivo [Diniz 2006].

Na prática o IoT é composto por diversos dispositivos que possuem capacidades restritas para tarefas de sensoriamento e comunicações em rede, tais como câmeras, sensores de movimento, lampadas, sensores térmicos entre outros. Dispositivos IoT fazem parte de nossas vidas diariamente, como nas casas, cidades, carros conectados, hospitais e indústria [Atzori et al. 2010]. No entanto a presença evasiva desses dispositivos podem gerar diversos riscos a privacidade dos usuários [Liu et al. 2018], onde a cada interação entre o usuário e estes dispositivos uma enorme quantidade de dados gerados são coletados sem seguir um padrão ou metodologia.

Junto a esta gama de novas possibilidades e alternativas criadas pela IoT, surgiram também novos desafios. Os desafios vão desde o desenvolvimento de aplicações que suportem a tecnologia embarcada nos dispositivos devido a sua restrição de tamanho, passando por questões de segurança como vazamento de informação e disponibilidade destes dispositivos [Al-Fuqaha et al. 2015]. Existem também muitas questões de padronização de protocolos de comunicação e intensa discussão sobre aspectos de privacidade e outras polêmicas socio técnicas. Aliado a estes desafios, e através de um viés voltado a Segurança da Informação (SI) buscando a privacidade, leis surgiram nos últimos anos, tendo por objetivo promover a proteção dos usuários quanto a suas informações pessoais na grande rede [Wachter 2018]. No entanto, estas leis também causam impactos sob o conceito do IoT, pois a atribuição de segurança requer uma maior capacidade dos dispositivos restritos, gerando assim desafios regulatórios.

No Brasil uma nova lei regulamentadora surgiu no segundo semestre de 2018, onde empresas de direito público e privado deverão estar de acordo até fevereiro de 2020. A lei em questão é a Lei Geral de Proteção de Dados [Casa Civil 2018], que visa proteger os dados pessoais e sigilosos dos usuários em relação as empresas que mantiverem estes dados. Neste contexto a IoT permite em muitos casos a identificação do usuário para controle de acesso, oferecendo uma infraestrutura básica para vincular estes da-

dos com a identidade dos usuários. Embora a LGPD ofereça orientações essenciais para regulamentação de serviços, deve-se buscar um equilíbrio entre o tratamento dos dados dos usuários e seus direitos de privacidade para estes dispositivos afim de não inviabilizar o uso destes dispositivos, sendo esta uma tarefa complexa.

De acordo com a LGPD todo usuário tem direito a privacidade e a proteção dos dados pessoais diante de empresas público/privadas juridicamente constituídas, no entanto este texto desafia a IoT em nichos como por exemplo a automação residencial, onde dispositivos estariam coletando uma gama de informações pessoais, aplicando algoritmos de inteligência artificial e ainda cruzando estas informações através de *Machine Learning* (ML) afim de gerar estatísticas para detectar padrões e comportamentos. Tais características compõem os principais objetivos de IoT no nicho de automação residencial, sendo os principais desafios; especificar métodos para coleta da autorização de uso dos dados do usuário pela empresa, padrões seguros para transmissão destes dados, modelos para promover o armazenamento seguro destas informações além de procedimentos para apagar todos os dados do usuário quando findado o relacionamento entre o mesmo e a empresa que coletou seus dados.

Neste sentido o presente artigo aborda em especifico os aspectos da Lei Geral de Proteção de Dados conhecida também pela sigla LGPD [Casa Civil 2018] relacionado ao uso de IoT, onde a lei busca através de seu texto reforçar a responsabilidade das empresas quanto ao uso e armazenamento dos dados de usuários. A responsabilidade exigida pode ser alcançada através da aplicação de mecanismos e técnicas da SI, onde a abordagem de muitos aspectos da lei esta diretamente relacionada a controles e modelos de privacidade de dados abordados por esta área.

O artigo esta organizado da seguinte forma. Na Seção 2 é apresentada a fundamentação teórica, trazendo conceitos de Segurança da Informação e IoT. Na Seção 3 a LGPD será descrita em maiores detalhes, na Seção 4 ocorre a análise entre LGPD e o universo de IoT utilizando aspectos da SI, finalmente na Seção 5 temos a conclusão.

## 2. FUNDAMENTAÇÃO TEÓRICA

O presente artigo expõe a preocupação relacionada aos riscos da privacidade dos usuários que utilizam dispositivos restritos de IoT. Embora a SI tenha evoluído para promover uma maior proteção em diversos dispositivos (incluindo móveis), isto nem sempre esteve diretamente relacionado a IoT devido a suas características.

Inúmeros ataques podem ser realizados devido as fragilidades das aplicações que utilizam hardwares restritos, expondo os usuários a preocupações relacionadas a LGPD. Tendo em vista que o conceito de SI está fortemente relacionado a proteção de um grupo de informações que buscam preservar o valor que estas possuem para uma pessoa ou organização, será abordado o item confidencialidade dentro da LGPD para IoT.

### 2.1. Segurança da Informação

O conceito de SI está fortemente relacionada a proteção de um grupo de informações que buscam preservar o valor que estas possuem para uma pessoa ou organização. Como complemento a essa definição, sendo os principais aspectos de segurança da informação definidos pela tríade da Confidencialidade, Integridade e Disponibilidade [Harris 2010]. Desta forma esta tríade é abordada como:

- **Confidencialidade** Visa garantir que somente quem deve acessar a informação de fato acesse a mesma.
- **Integridade** Tem o intuito de garantir que a informação acessada realmente está correta, integra, não foi modificada ou alvo de fraude/falsificação.
- **Disponibilidade** Visa garantir que a informação possa ser obtida sempre que for necessário, assim, estando sempre disponível para quem necessite fazer uso da mesma.

O princípio que gera a privacidade em SI é a confidencialidade, onde segundo [Sêmola 2014] menciona: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas a quem é destinada.

Como fundamentação da SI temos o conjunto de normas da família ISO 27000 que traz diversos conceitos afim de se obter uma maior segurança das informações através de um Sistema de Gestão de Segurança da Informação (SGSI) para uma organização. As normas são referências de segurança trazendo consigo uma serie de controles, boas práticas e um conjunto de mecanismos para garantir continua de revisão e melhoria nos processos de negócio a fim de evitar percas para uma companhia [Oliveira et al. 2016]. Estas normas devem ser utilizadas como base para a segurança da informação quando houver necessidade de tratar-se deste tema.

As limitações devidas a baixa capacidade dos dispositivos IoT não devem ser interpretados apenas como um problema, mas peça chave no correto manuseio da mesma. A SI é abrangente no sentido de soluções a fim de garantir os pilares básicos aqui descritos. Um controle pode ser desde um recurso técnico de TI, como um procedimento ou verificação ou a sua frequência de ocorrências [Repinoski and Morães 2018]. A simples utilização de um log de ações por exemplo, já configura um item de segurança para um determinado dispositivo, em virtude das informações que ali se encontram. Isto pode ser verificado também quando processos e atividades são documentadas, sendo estas caracterizadas como controles da gestão de conhecimento que visando a garantia da continuação dos processos de uma organização.

Em geral, no momento da concepção de um novo modelo de negócio onde a SI é negligenciada, cria-se um desafio para a existência e continuidade do mesmo, pois a SI envolve diversos campos da tecnologia e documentação, assim como possui estrita ligação com setores jurídicos e de RH das organizações. Razão esta que a SI tem maior afinidade ao assunto aqui relacionado e seus desafios.

### 2.2. Internet das Coisas (IoT)

Um número cada vez maior de objetos físicos está sendo conectado à Internet a uma velocidade sem precedentes, atribuindo a estes a ideia da IoT [Al-Fuqaha et al. 2015]. Muitos dispositivos os quais normalmente não se conectavam a rede, estarão presentes, podendo coletar dados, gerar informações para análises e monitoramentos, bem como automatizar tarefas ou prover alguma facilidade ao usuário, tais dispositivos denominam-se, restritos [SINGER 2012]. A Figura 1 demonstra um o conceito geral da IoT onde existe uma interação dos serviços realizados com os domínios específicos.

Conforme [Santos et al. 2016], a IoT pode prover diversas classes de serviços, dentre elas, destacam-se os serviços de identificação, responsáveis por mapear entidades


**Figura 1. Demonstração da IoT enfatizando os mercados verticais e as integração horizontal entre eles [Al-Fuqaha et al. 2015]**

físicas (de interesse do usuário), entidades virtuais (EV) como, por exemplo, a temperatura de um local físico, coordenadas geográficas e serviços de agregação de dados que coletam e sumarizam dados obtidos dos objetos inteligentes, entre tantos outros segmentos.

Dispositivos restritos, é a principal nomenclatura utilizada para descrever os atores a serem utilizados em internet das coisas que possuem limitações físicas de *hardware*. Sendo estas limitações grandes barreiras no contexto de recursos computacionais, como memória, processador, armazenamento, energia e a transmissão de dados. Desta forma, toda implementação deve ser bem planejada onde normalmente apresentam um problema complexo. Este ponto cria um grande desafio de SI para dispositivos IoT, devido a escassez de recursos computacionais, onde além da funcionalidade do dispositivo, adicionar novos recursos para segurança normalmente é visto como oneroso ao projeto. No entanto, a LGPD através de seu viés regulatório tem meios para exigir estes recursos ao projeto devido ao seu peso de lei, embora isto nada mude o fato de ainda ser um desafio no desenvolvimento de uma solução IoT.

As denominadas “coisas”ou seja, os dispositivos, irão operar em todas as camadas do tradicional modelo de rede, assim, não mais apenas um tradicional computador ou notebook estarão utilizando a pilha TCP/IP, por exemplo, agora também um sensor através de um pequeno dispositivo com Arduíno[1] em uma sala poderá acessar todas as camadas, estando este exposto a vulnerabilidades e vazamento de informações. É possível verificar

[1] Arduíno é uma plataforma de prototipagem eletrônica de hardware livre e de placa única, projetada com um microcontrolador com suporte de entrada/saída embutido, utilizando uma linguagem de programação padrão, a qual tem origem em Wiring, e é essencialmente C/C++

que o modelo de camadas está presente desde o enlace passando pela rede, incluindo IPv6, podendo chegar até o nível de aplicação, onde isto ocorre através de protocolos adaptados e pensados para necessidades de IoT (baixa largura de banda, poucos recursos computacionais e de energia).

Cada dispositivo no universo de IoT pode ser classificado em uma classe, de acordo com sua capacidade de memória e armazenamento de código. As classes são, por sua vez, definidas em 0, 1 e 2 [Bormann 2014]. Classe 0, possui restrição muito alta, usada apenas como sensor. A classe 1, ainda possui restrição alta, porém, já permite operar com o cabeçalho TCP e protocolos adaptados para ambientes restritos como CoAP [Shelby 2014], etc. Por fim, a classe 2 possui uma maior capacidade se comparada as anteriores, onde inclusive pode operar com mais de um protocolo a nível de aplicação.

A Tabela 1, ilustra o modelo de camadas com alguns exemplos de seus componentes. Vale ressaltar que tecnologias emergentes, promessas e ideias para o futuro estão em andamento, de tal modo, não há um padrão único adotado de desenvolvimento para cada camada, onde muitas vezes é necessário um entendimento do todo (aplicação e tecnologia) com o intuito de encontrar quais protocolos em cada parte do modelo podem atender melhor a respectiva demanda. Não há um padrão ideal a ser a dotado de protocolos em todas as camadas, sendo necessário análise do cenário a ser aplicado.

**Tabela 1. Estrutura IoT**

| CAMADA | TECNOLOGIA OU PROTOCOLO | CLASSE DO DISPOSITIVO |
|---|---|---|
| APLICAÇÃO | CoAP, MQTT, AMPQ, XMPP | C1, C2 |
| TRANSPORTE | TCP / UDP | C1, C2 |
| REDE | 6LoWPAN, IPv4, IPv6 | C1, C2 |
| ENLACE | RFID, NFC, Bluetooth, Ble, Z-wave, Wifi IEEE 802.15.4, GSM | C0, C1, C2 |
| FÍSICA | Arduino, Raspberry, Beagle Done, Smartphones | C0, C1, C2 |

Fonte: Elaborado pelo autor.

## 3. Lei Geral de Proteção de Dados Pessoais

Visando fortalecer a proteção das informações pessoais e a transparência na forma de tratamento e armazenamento de dados, foi sancionada parcialmente, com alguns vetos, pelo Presidente da República Michel Temer, no dia 14 de agosto de 2018, a lei Nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD) [Agostinelli 2018].

Embora o país já disponha de mais de 40 normas que direta e indiretamente tratavam da proteção à privacidade e aos dados pessoais, a LGPD criou um novo modelo de regras para o uso de dados pessoais para o âmbito online e offline nos setores públicos e privados. Todavia, a LGPD vem a complementar esse marco regulatório setorial, que por vezes era conflituoso, trazendo insegurança jurídica e deixando o país menos competitivo no contexto de uma sociedade cada vez mais movida a dados [Casa Civil 2018].

Dentre os diversos artigos e parágrafos identificados no texto da LGPD, podemos citar como sendo os mais relevantes para este trabalho os seguintes itens:

- **Uso da Informação:** Especificar para o usuário qual a finalidade da coleta de seus dados, além de ser transparente em relação ao tratamento dessas informações e adotar medidas que garantam sua segurança;
- **Acesso a Informação:** O usuário deve ter acesso fácil às informações que estão sendo utilizadas sempre que desejar, podendo revogar seu consentimento de compartilhamento de dados posteriormente, sem maiores dificuldades;
- **Titularidade e Responsabilidade:** O ”titular”dos dados é a pessoa a qual as informações se referem. No entanto, quando o titular concorda com o uso de suas informações, a empresa torna-se a responsável pela sua segurança e seu tratamento;
- **Tratamento das Informações:** O tratamento de dados deve ser finalizado quando o objetivo especificado anteriormente for alcançado (salvo casos específicos), quando as informações deixarem de ser necessárias ou quando o órgão regulador solicitar;
- **Divulgação de Incidentes:** Qualquer vazamento ou falha de segurança que comprometa os dados de algum usuário devem ser relatados imediatamente às autoridades competentes, para que o problema seja resolvido.

Estes pontos buscam estabelecer regras claras para empresas sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, fomentando desta forma o desenvolvimento econômico e tecnológico numa sociedade movida a dados [AGOSTINELLI 2018]. Além disto a LGPD busca fortalecer a confiança da sociedade quanto ao uso de seus dados coletados por terceiros através de um respaldo jurídico alcançado por esta lei.

Através dos itens citados a LGPD busca tornar-se responsável por algumas vantagens quanto ao processamento de dados em território brasileiro ou dados coletados dentro do pais, facilitando a vida da sociedade. Para tanto, a LGPD estabeleceu regras únicas e harmônicas sobre o uso de dados pessoais, independente do setor da economia, atribuindo uma maior flexibilidade para o tratamento de dados pessoais em casos de legítimo interesse visando uso de conceitos como Big Data[2]. É possível observar que a LGPD também visa reduzir custos operacionais causados por incompatibilidades sistêmicas de tratamentos feitos por agentes diversos, além de fomentar uma maior qualidade dos dados em circulação no ecossistema como um todo. Assim o Brasil torna-se apto a processar dados oriundos de países que exigem um nível de proteção de dados adequados, o que pode fomentar principalmente, os setores de tecnologia da informação facilitando a portabilidade dos dados de um serviço para outro, aumentando a competitividade no mercado.

A LGPD ao todo possui 65 artigos, que expõe a preocupação com a privacidade dos dados. Conforme mencionado tal existência da lei atribui por sí só uma maior competitividade ao pais, pois alguns nichos de mercado e países possuem evidentes preocupações com o devido tratamento de suas informações. Deste modo o Brasil viu esta necessidade de estar em conformidade com o restante dos países afim de se tornar-se mais competitivo afim de realizar mais negócios em um cenário internacional.

[2]Big Data é a análise e a interpretação de grandes volumes de dados de grande variedade. Isto permite que profissionais de TI possam trabalhar com informações não-estruturadas a uma grande velocidade.

## 4. Segurança da Informação, LGPD e IoT

Evidenciado o objetivo de manter a privacidade dos dados de usuários através do texto trazido pela LGPD, verificam-se os desafio direcionados a aplicação dos mecanismos e tecnologias afim de atingir estes objetivos em dispositivos que por padrão possuem limitações físicas. Dispositivos IoT utilizados dentro de residências (lâmpadas, cortinas, sensores de presença, fechadura eletrônica, ar condicionado, etc..), em veículos ou em qualquer atividades de uso diário, atualmente já coletam informações sobre o comportamento e o perfil dos usuários. Os dados coletados podem inferir padrões de comportamento e horários de utilização de recursos, sendo estas informações consideradas como pessoais e em alguns casos até sigilosa onde os usuários têm total direito a privacidade das mesmas. Nestes casos, um certo esforço precisa ser empreendido para atingir os objetivos da LGPD.

Em situações de coleta, transmissão e armazenamento das informações dos usuários, são necessários considerar alguns pontos para implementar os requisitos de segurança em dispositivos restritos devido as suas características físicas identificadas: baixa capacidade de processamento dos dispositivos, vida útil da bateria menor, memória e armazenamento dos dispositivos limitadas, tamanho de pacotes menores e uma largura de banda reduzida [Sethi et al. 2018]. Desta forma a SI pode ser utilizada através de suas normas para atingir os objetivos da LGPD, onde esta família de normas suportam os pontos identificados na lei.

A exemplo a LGPD menciona através de seus artigos regras explicitas quanto o ciclo de vida da informação, ou seja, sua coleta, armazenamento, tratamento, compartilhamento e descarte. Este ponto tem como principal objetivo fortalecer a confiança na sociedade (verificável através da norma [ISO 27001 2013]), que atribui respaldo jurídico sobre normatização e preocupação com a informação, juntamente com todo um mapeamento do seu ciclo de vida. O processo de gestão de incidentes e comunicação dos mesmos, pois conforme a LGPD todo incidente relacionado a privacidade dos usuários deverá ser comunicado (suportado pela norma [ISO 27002 2013]). Procedimentos como mapeamento de processos nas organizações, entendimento dos mesmos e análise de vulnerabilidades destes seguidos de revisão nos processos de classificação e ações contra o vazamento da informação, precisarão ser mapeados e atualizados no ambiente de SI para conformidade com a LGPD (suportado pela norma [ISO 27005 2011]).

Desta forma é possível reduzir casos onde a SI acaba sendo negligenciada nos projetos os quais só o simples fato de operar e ser funcional já se mostra um desafio em IoT, principalmente em equipamentos classe C0 e C1.

### 4.1. Coleta

Tratando-se do processo de coleta, alguns itens necessitam ser observados para que se esteja em conformidade com a LGPD descritas no primeiro artigo desta. A lei especifica que qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos. Para isto os dados pessoais objeto do tratamento devem ser coletados em território nacional ou cujo titular nele se encontre no momento da coleta.

Logo os controladores e operadores das informações coletadas, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização. Estas práticas podem ter como referências a família da ISO 27000 onde mais especificamente a [ISO 27002 2013] aborda os controles que podem ser aplicados afim de obter-se estas práticas.

Outros pontos precisam estar claros e definidos também, sendo estes; o regime de funcionamento, os procedimentos (incluindo reclamações e petições de titulares), as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Todos estes procedimentos podem ser atingidos através de boas práticas instauradas pela governança dos controladores e operadores de informações coletadas.

Desta forma, verifica-se a necessidade de disponibilizar mecanismos que indiquem ao usuário a finalidade da coleta de suas informações e ainda se este autoriza a coleta destes dados. Não sendo isto transparente para o usuário, os dados ali coletados não poderão ser utilizados, pois isto contrariaria a LGPD e a pessoa jurídica de direito público ou privado poderia ser penalizada conforme as multas descritas no capítulo 8, Sanções Administrativas, artigo 52º da referida lei [Casa Civil 2018].

### 4.2. Transmissão

A transmissão dos dados utilizadas em muitos dispositivos requer também mecanismos de controle e segurança afim de estar em conformidade com a LGPD. O maior desafio ocorre por conta dos dispositivos de classe 0, que apenas coletam algo e enviam utilizando tecnologia sem fio de baixo consumo de energia, tais equipamentos não possuem recursos para executarem, por exemplo, a pilha TCP/IP e protocolos adaptados para internet das coisas na camada de aplicação.

No entanto, em caso de um cenário hibrido onde podem coexistir equipamentos de classe um ou dois, os quais suportam protocolos como CoAP e outros por exemplo, seria necessário a integração entre os ambos. Nestes cenários a opção de utilização de gateways seria uma alternativa, onde determinados equipamentos de um fabricante ou classe realizam a comunicação e o envio de informações para um ponto comum na rede o qual irá fazer o tratamento desta, traduções ou modificações se necessárias e, também permitir implementações as quais estes dispositivos não seriam capazes devido a sua restrição. Esta utilização de gateways em um primeiro momento pode permitir centralizar informações, auxiliar nas dificuldades de escassez de recursos computacionais, porém trazem consigo acréscimo na topologia, bem como mais pontos adicionais para vulnerabilidades.

Contudo o tráfego destas informações necessita de uma camada extra de segurança, afim de evitar que uma interceptação de mensagens dentro de uma rede possa ser realizada e seus dados expostos. A LGPD traz em seu artigo 6º referencias relacionadas à segurança neste assunto, destacando a necessidade de utilizar medidas técnicas e administrativas para proteger os dados pessoais e sigilos, contra acessos não autorizados e de situações acidentais, ilícitas de destruição, perda ou alteração na comunicação e difusão dos dados.

No processo de transmissão da informação, os dispositivos restritos podem estar operando com 6lo na camada de rede, no entanto, a camada inferior, onde a comunicação sem fio pode ser utilizada de modo aberto traz um ambiente exposto a ataques, capturas de pacotes e a exploração de vulnerabilidades. Nestes casos diversos ataques podem ser realizados contra as informações que trafegam entre as camadas OSI.

### 4.2.1. Tipos de Ataques a Transmissão

Diversos tipos de ameaças direcionadas a uma camada específica na pilha de protocolos de um dispositivo utilizando 6Lo podem ser realizadas, estes ataques ocorrem desde a camada física de link de dados, até a camada de aplicação ou ainda uma combinação de qualquer uma das camadas do modelo OSI. Em nosso documento buscamos descrever ataques relacionados a camada de rede, camada esta onde opera o protocolo IPv6 modificado para uso em dispositivos de hardware restrito (6Lo). A camada de rede nestes dispositivos, notoriamente e a que sofre a maioria dos ataques, estes ataques são:

Injeção de mensagens. Este tipo de ataque possui características iguais a famigerada exploração do homem do meio, imputando pacotes no protocolo da camada inferior, IEEE 802.15.4 [Kivinen 2017],que por sua vez, é o padrão adotado para desenvolvimento de tecnologias sem fio em dispositivos restritos pelo IEEE, fazendo utilização de outro dispositivo ou host no meio do caminho, tais pacotes serão encaminhados ao destino final para serem processados.

No momento da resposta, esta informação será recebida pelo dispositivo fraudulento no meio do caminho e o mesmo trata de encaminhar para origem os pacotes, transmitindo a sensação a respeito de um fluxo normal na comunicação. A Figura 2 demonstra este tipo de ataque onde há interação do interceptador no meio do caminho.

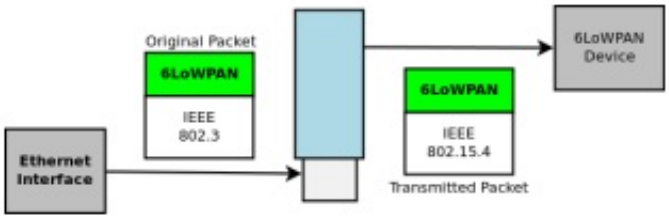


**Figura 2. Ataque de injeção de mensagens, similar ao homem do meio [Lahmadi 2014]**

Em outro exemplo podem ocorrer ataques do tipo fragmentação de pacotes, sendo estes utilizado para dividir uma carga de dados em diversas partes menores. A remontagem de pacotes em dispositivos restritos pode gerar problemas como processamento extra e consequentemente um consumo maior de energia desligando este equipamento, além de também esquentar o dispositivo. Logo, ameaças muitas vezes superadas em um ambiente tradicional, surgem no ambiente restrito com maior potencial ofensivo, por exemplo; ping da morte e sobreposição de fragmentos de pacotes, conhecido como *Teardrop*, são exemplos de ataque que podem explorar estas vulnerabilidades em dispositivos restritos.

Desta forma, após a coleta dos dados devem ser tomadas algumas ações durante

a transmissão até estas estejam em seu armazenamento final para manter conformidade com a LGPD. Estas ações sugerem a utilização de técnicas seguras do ambiente convencional de computação que deverão ser aplicadas neste cenário, assim controles como VPNs com a utilização de protocolos e chaves criptográficas podem ser utilizados em dispositivos mais robustos, gateways e concentradores de rede, permitindo maior poder computacional.

### 4.3. Armazenamento

Um dos desafios relacionado a IoT quanto a segurança de seus usuários é a forma como estes dados deverão ser protegidos, uma vez que não existe muitas possibilidades para alterações físicas destes dispositivos afim de empregar os requisitos vistos na LGPD. Como alternativa, os dados armazenados podem ser passiveis de criptografia afim de aumentar a segurança dos usuários, principalmente informações sobre dados sigilos. No entanto técnicas criptográficas poderiam consumir recursos altos para execução desta tarefa.

Cenários onde o usuário solicitasse a exclusão ou extração de todos seus dados, exigiria grandes custos para consulta ou exclusão das informações relacionadas ao usuário, em caso de armazenamento no próprio dispositivo. Este exemplo pode ser verificado no artigo 9º da LGPD onde informa que a confirmação de existência ou o acesso a dados pessoais deverão ser providenciadas, mediante requisição do titular, onde estes devem estar em formato simplificado para disponibilização imediata, sendo estas através de meio eletrônico, seguro e idôneo para esse fim. Estas solicitações de informação podem ocorrer a qualquer tempo, logo estes dados precisam ser organizados em um formato que favoreça o exercício do direito de acesso, implicando em recursos extras em um ambiente restritos para armazenamento destes dados.

Sob o aspecto da SI, este ponto referente a disponibilidade das informações de maneira imediata, impacta por exemplo nos controles que visam evitar o vazamento destes dados protegendo a borda da rede, assim como demais passos utilizados pela informação durante seu ciclo de vida.

Logo é torna-se indispensável promover a proteção dos dados pessoais e sigilosos armazenado em IoT, contudo tratando-se de ambientes onde os recursos do hardware são limitados, inviabilizasse a utilização de criptografias tradicionais, onde a execução de algoritmos criptográficos teria um alto custo, degradando o desempenho computacional e o alto consumo de energia.

#### 4.3.1. Segurança no Armazenamento por meio da Criptografia

Tratando-se de ambientes onde os recursos do hardware são limitados (dispositivos restritos) em relação à capacidade de processamento, memória e consumo de energia devido ao seu tamanho, é usual separar as informações importantes dos demais dados. A separação dos dados implica em sua classificação de acordo com o seu grau de valor ou significado que o conjunto de dados possui, onde estas informações consideradas sensíveis devem receber uma proteção criptográfica [TACHIBANA 2017].

No entanto a LGPD em seu texto relaciona dados pessoais e dados sigilosos como classificações que necessitam de proteção. Deste modo podem ser utilizadas como alter-

nativas para a criptografia destes dados cifras de blocos leves. Neste modelo não há necessidade de classificação dos dados, tornando-se uma boa alternativa para atingir níveis de proteção desejáveis pela LGPD em dispositivos restritos sem degradar seu desempenho computacional.

Cifras de blocos leves baseiam-se em funções de rede de Feistel e Substituição de Permuta. Este tipo de cifra, funciona com a execução de uma função de mapeamento de blocos possuindo n-bits de texto não cifrado para blocos de n-bits de texto cifrado, onde "n"é comprimento do bloco. Parametrizada por k-bits, a função da chave "K"contém o mesmo tamanho do bloco, impossibilitando a expansão dos dados [Katz et al. 1996].

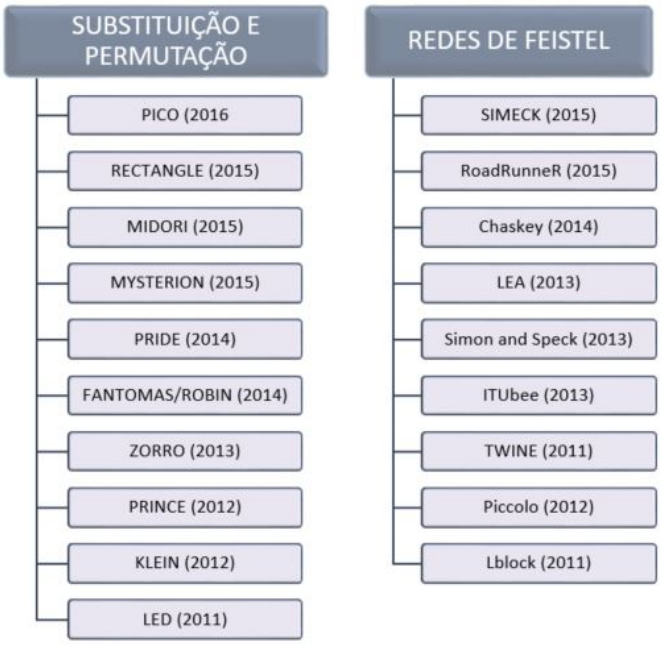


**Figura 3. Relação de algoritmos de cifras leves dos últimos seis anos [TACHIBANA 2017]**

Evidentemente a redução de poder da criptografia de cifras de blocos leves diminui os níveis de segurança em relação a algoritmos mais robustos como o Advanced Encryption Standard (AES) em sua aplicabilidade original, porem atualmente a maioria das informações são armazenadas em texto claro e a aplicação de uma criptografia de cifras de blocos leves já traria um ganho significativo a segurança.

## 5. Conclusão

Este trabalho compreendeu-se em discutir soluções e alternativas para conformidade da Lei Geral de Proteção de Dados (LGPD) através da Segurança da Informação (SI) em dispositivos restritos IoT. Verificou-se que a SI demonstra alta relevância neste contexto, servindo como base para atingir os requisitos legais verificados no texto da LGPD. Assim foram abordados os principais aspectos da lei sendo discutido as soluções disponíveis para IoT verificáveis na SI nos métodos de coleta, transmissão e armazenamento dos dados.

Primeiramente foram apresentadas as fundamentações relacionados a temática proposta. Sendo abordados posteriormente as contribuições para atingir os principais

pontos de conformidades descritas no texto da LGPD, onde foram avaliados os cenários de aplicação desta legislação em dispositivos restritos. Como resultado, o trabalho procurou recuperar soluções identificadas na literatura existente referente a aplicação e impacto dos mecanismos e tecnologias relacionados a privacidade dos usuários que utilizam dispositivos restritos IoT.

Como pode-se observar, são grandes os desafios do tema proposto devido a complexabilidade de aplicar requisitos de segurança a objetos com processamento, memoria, largura de banda e energia restritos. Ainda assim, independentemente do cenário de IoT que este estará compreendido, a aplicabilidade destes mecanismos e tecnologias descritas neste trabalho deverão empregar uma maior proteção aos usuários quanto a seus dados. Diminuindo assim as lacunas presentes entre a LGPD e a SI para dispositivos restritos.

## Referências


AGOSTINELLI, J. (2018). A importância da lei geral de proteção de dados pessoais no ambiente online. *ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498*, 14(14).

Agostinelli, J. (2018). A importância da lei geral de proteção de dados pessoais no ambiente online. *São Paulo: Toledo centro universitário*.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376.

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15):2787–2805.

Bormann, C. (2014). Terminology for Constrained-Node Networks. RFC 7228, RFC Editor.

Casa Civil, d. B. (2018). Lei nº 13.709, de 14 de agosto de 2018. `http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm`. [Online; acesso 03-Oct-2018].

Diniz, E. H. (2006). Internet das coisas. *GV-executivo*, 5(1):59.

Forbes (2014). A simple explanation of 'the internet of things). `https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1a4fb9791d09`. [Online; acesso Dez-2018].

Harris, S. (2010). *CISSP All-in-one Exam Guide, McGraw Hill Professional*. Módulo.

IBGE (2017). Assinantes telefonia celular. disponível em:. `https://paises.ibge.gov.br/#/pt/pais/brasil/info/redes`. [Online; acesso 08-Dez-2018].

ISO 27001 (2013). Information technology – security techniques – information security management systems – requirements. Standard, International Organization for Standardization.

ISO 27002 (2013). Information technology — security techniques — code of practice for information security controls. Standard, International Organization for Standardization.

ISO 27005 (2011). Information technology - security techniques - information security risk management. Standard, International Organization for Standardization.

Katz, J., Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

Kivinen, T. (2017). IEEE 802.15.4 Information Element for the IETF. RFC 8137, RFC Editor.

Lahmadi, A. (2014). A testing framework for discovering vulnerabilities in 6lowpan networks. *University of Lorraine*.

LEMOS, A. and MARQUES, D. (2018). Questões sobre privacidade na internet das coisas. *Congresso do INCT.DD*.

Liu, J., Zhang, C., and Fang, Y. (2018). Epic: A differential privacy framework to defend smart homes against internet traffic analysis. *IEEE Internet of Things Journal*, 5(2):1206–1217.

Oliveira, M. S., Peixoto, S. C., Santos, A. F., Maniçoba, R. H. C., and Guimarães, M. A. (2016). Aplicação das normas abnt nbr iso/iec 27001 e abnt nbr iso/iec 27002 em uma média empresa. *Revista Eletrônica de Sistemas de Informação e de Gestão Tecnológica*, 6(2).

Oulasvirta, A., Rattenbury, T., Ma, L., and Raita, E. (2012). Habits make smartphone use more pervasive. *Personal Ubiquitous Comput.*, 16(1):105–114.

Repinoski, B. C. and Morães, M. J. F. (2018). A implementação da iso/iec 27002 em uma empresa. *Anais do EVINCI-UniBrasil*, 3(1):328–328.

Santos, B. P., Silva, L., Celes, C., Borges, J. B., Neto, B. S. P., Vieira, M. A. M., Vieira, L. F. M., Goussevskaia, O. N., and Loureiro, A. (2016). Internet das coisas: da teoriaa prática. *Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos*.

Sêmola, M. (2014). *Gestão da segurança da informação*, volume 2. Elsevier Brasil, Rua da Assembléia, 100 - 6º andar Centro - Rio de Janeiro - RJ - Brasil – CEP: 20011-904.

Sethi, M., Arkko, J., Keranen, A., and Back, H. (2018). Practical considerations and implementation experiences in securing smart object networks. Technical report.

Shelby, Z. (2014). The Constrained Application Protocol (CoAP). RFC 7252, RFC Editor.

SINGER, T. (2012). Tudo conectado: conceitos e representações da internet das coisas. *Simpósio em tecnologias digitais e sociabilidade*, 2:1–15.

TACHIBANA, FERNANDA OHNUMA, M. (2017). Implementação em hardware e sistemas embarcados de algoritmos de criptografia leve para aplicação em iot.

Wachter, S. (2018). Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the gdpr. *Computer law & security review*, 34(3):436–449.

World IPv6 Launch, W. (2018). World ipv6 launch. infographic. disponível em:. `https://www.worldipv6launch.org/infographic/`. [Online; acesso 08-Dez-2018].