Revista Tecnologia
Universidade de Fortaleza
e-ISSN: 2318-0730

10.5020/23180730.2024.13998

Desafios Regulatórios da Lei Geral de Proteção de Dados (LGPD) para Internet das Coisas (IoT)

Regulatory challenges of the General Personal Data Protection Law (LGPD) for the Internet of Things (IoT)

Desafíos Regulatorios de la Ley General de Protección de Datos (LGPD) para la Internet de las Cosas (IoT)

Antonio Alisio de Meneses Cordeiro
Serviço Federal de Processamento de Dados - Serpro, Fortaleza, Ceará, Brasil
alisio.meneses@gmail.com

Leandro Lima Sobral
G4 Flex Business Services, Fortaleza, Ceará, Brasil
eules.leandro@gmail.com

Resumo

Nos últimos anos, os objetos inteligentes com capacidade de detecção, processamento e comunicação proliferaram. A Internet das Coisas (IoT) conecta esses objetos à internet e fornece comunicação entre usuários e dispositivos. A IoT promove inovações das quais toda a sociedade pode se beneficiar, como cidades inteligentes, saúde e automação. Por outro lado, precisamos resolver vários problemas sociais, teóricos e práticos. Para atender a estas questões, é necessário transpor barreiras como a garantia da privacidade dos dados, as restrições de capacidade de processamento, memória e consumo de energia de dispositivos restritos, e os desafios normativos e regulatórios. Este artigo tem como objetivo analisar os desafios da segurança de informação da IoT sob o prisma da Lei Geral de Proteção de Dados (LGPD), com foco na proteção dos direitos fundamentais de liberdade e de privacidade do povo brasileiro. A metodologia adotada consistiu em uma revisão de literatura especializada, contemplando artigos, normas e estudos de caso publicados sobre o tema. Como principais constatações, identificou-se que a formulação e adoção de boas práticas e regras de governança por parte dos controladores e operadores de dados, a utilização de *gateways* em redes isoladas para dispositivos IoT e o emprego de algoritmos leves para cifrar dados armazenados constituem, atualmente, maneiras viáveis de prover melhor segurança aos dados dos usuários e de atender às exigências da LGPD.

Palavras-chave: cibersegurança; internet das coisas; proteção de dados pessoais; lei geral de proteção de dados; governança de dados.

Abstract

In recent years, smart objects with sensing, processing, and communication capabilities have proliferated. The Internet of Things (IoT) connects these objects to the Internet and provides communication between users and devices. IoT promotes innovations that can benefit society as a whole, such as smart cities, healthcare, and automation. On the other hand, we need to solve several social, theoretical, and practical problems. To address these issues, it is necessary to overcome barriers such as ensuring data privacy, restrictions on processing capacity and memory, energy consumption of restricted devices, and normative and regulatory challenges. This article aims to analyze the IoT information security challenges from the General Personal Data Protection Law (LGPD) perspective, focusing on protecting the Brazilian people's fundamental rights of freedom and privacy. The methodology adopted consisted of a review of specialized literature, including articles, standards, and case studies published on the issue. As main findings, it was identified that the formulation and adoption of good practices and governance rules by data controllers and operators, the use of gateways in isolated networks for IoT devices, and the use of lightweight algorithms to encrypt stored data currently constitute viable ways to provide better security to user data and meet the requirements of the LGPD.

Keywords: *cybersecurity; internet of things; personal data protection; general data protection law; data governance.*

Resumen

En los últimos años, los objetos inteligentes con capacidad de detección, procesamiento y comunicación se han proliferado significativamente. La Internet de las Cosas (IoT, por su sigla en inglés) conecta dichos objetos a la internet y permite la comunicación entre usuarios y dispositivos. La IoT impulsa innovaciones de las que toda la sociedad puede beneficiarse, tales como las ciudades inteligentes, la atención médica y la automatización. No obstante, es imprescindible resolver diversos problemas sociales, teóricos y prácticos. Para enfrentar estos desafíos, es necesario superar barreras como la garantía de la privacidad de los datos, las limitaciones de capacidad de procesamiento, memoria y consumo energético de dispositivos restringidos, así como los retos normativos y regulatorios. Este artículo tiene como objetivo analizar los desafíos relacionados con la seguridad de la información en el contexto de la IoT, desde la perspectiva de la Ley General de Protección de Datos (LGPD), con énfasis en la salvaguarda de los derechos fundamentales de libertad y privacidad del pueblo brasileño. La metodología adoptada consistió en una revisión de la literatura especializada, incluyendo artículos, normas y estudios de caso publicados sobre la temática. Entre los principales hallazgos, se identificó que la formulación y adopción de buenas prácticas y normas de gobernanza por parte de los controladores y operadores de datos, el uso de gateways en redes aisladas para dispositivos IoT y la implementación de algoritmos ligeros para el cifrado de datos almacenados constituyen, actualmente, alternativas viables para mejorar la seguridad de los datos de los usuarios y cumplir con los requisitos establecidos por la LGPD.

Palabras clave: *ciberseguridad; internet de las cosas; protección de datos personales; Ley General de Protección de Datos; gobernanza de datos.*

1 Introdução

O rápido crescimento no uso de dispositivos de Internet das Coisas (IoT) será transformador para todos os tipos de organizações, com expectativa de crescimento do mercado para mais de 2,4 trilhões de dólares anualmente até 2027. Os pontos-chave para estas projeções são a adoção de redes 5G, inteligência artificial e aprendizado de máquina (Newman, 2020).

> A IoT é definida por conexões e serviços vinculados, ajustados às necessidades específicas dos usuários. Objetos e serviços devem ser conectados uns aos outros e compartilhar dados sobre um usuário específico para fornecer serviços em rede que são informados por mais do que a interação direta do usuário com um nó específico. Sem a identificação repetida e consistente de usuários, serviços integrados e contínuos não seriam possíveis (Wachter, 2018, tradução nossa).

As aplicações de IoT são variadas e as casas inteligentes e inovações em saúde estão entre as mais promissoras. As casas inteligentes podem fazer uso de câmeras de vigilância, sensores de presença, termostatos, entre outros dispositivos, possibilitando detecção abrangente e podendo ser controladas remotamente por donos de casa ou cuidadores (Liu; Zhang; Fang, 2018, tradução nossa). Além desta, a IoT está inovando a área da saúde através de detecção de ataques cardíacos, soluções para pessoas com asma, proteção de dados, monitoramento de sinais vitais e de pacientes com mal de Parkinson, e detecção de quedas (Rodrigues Neto, 2020).

Empresas investem em tecnologias que utilizam essas informações, como inteligência artificial, *big data* e *machine learning* para o oferecimento de produtos e serviços de acordo com a necessidade dos clientes. A constante vigilância proporcionada pelos dispositivos tecnológicos, a grande quantidade de dados e a possibilidade de recuperação destes dados por outros usuários e aplicações constituem ameaças à privacidade do indivíduo (Affonso, 2018), dados estes cuja coleta não segue um padrão ou metodologia (Oliveira *et al.,* 2019).

A relevância do tema está na urgência de analisar o impacto da IoT em relação à privacidade e a proteção de dados pessoais, particularmente diante dos desafios ocasionados pela Lei Geral de Proteção de Dados (LGPD). A motivação deste estudo reside no aumento do risco da exposição de dados sensíveis, decorrente da crescente adoção de dispositivos IoT, evidenciando a necessidade de atender às exigências legais estabelecidas

para a proteção de dados pessoais. A LGPD constitui o principal marco regulatório brasileiro para orientar práticas de coleta, transmissão e armazenamento de dados pessoais em ambientes tecnológicos no cenário brasileiro (Brasil, 2018).

No Brasil, a Lei Geral de Proteção de Dados, que entrou em vigor em 2020, é a principal regulamentação do Brasil destinada à proteção de dados pessoais. Essa Lei dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado. A LGPD define como informações relacionadas à pessoa natural identificada ou identificável. Os dados sensíveis são aqueles que revelam origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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 (Brasil, 2018).

A LGPD se aplica a todas as organizações, estabelecidas ou não no Brasil, que processam dados pessoais para prestar bens ou serviços ao povo brasileiro. LGPD também se aplica a organizações que coletam ou processam dados pessoais no Brasil (Amazon Web Services, s.d.).

A proteção dos sistemas de IoT traz desafios particulares à medida que cresce a demanda pela tecnologia, sendo implementados em ambientes sem padrão definido, complexos e frequentemente hostis, passando por questões de quantidades limitadas de armazenamento, memória e capacidade de processamento, proteção de comunicação e gestão de vulnerabilidades (Gerber; Kansal, 2020), fatos que criam desafios regulatórios. Este trabalho tem como objetivo analisar os desafios regulatórios ocasionados pela aplicação da LGPD, no contexto da segurança da informação em dispositivos de IoT (Oliveira; Vega, 2024). A análise busca identificar os principais entraves técnicos e normativos, considerando as limitações dos dispositivos, e propor soluções que promovam a conformidade legal e assegurem a proteção dos dados pessoais.

O artigo está organizado da seguinte maneira: seção 1: introdução (previamente apresentada); seção 2: fundamentação teórica onde são apresentados conceitos de segurança de informação e IoT; seção 3: descrição da Lei Geral de Proteção de Dados, análise no contexto de IoT e segurança da informação, e desafios da segurança da informação em IoT sob o prisma da LGPD; seção 4: conclusão.

2 Fundamentação teórica

2.1 Segurança de informação

O dado é um objeto ou fato bruto percebido pelo sujeito, não construído nem elaborado na consciência, sem passar por processos de análise ou avaliação para sua transferência como informação. A informação é um fenômeno gerado a partir do conhecimento, analisado e interpretado para que seu conteúdo seja significativo (Pinheiro. s.d., *apud* Zins, 2007).

Dentre os principais conceitos de segurança de informação, podemos dar ênfase a três aspectos de maior importância, conhecidos como a Tríade da segurança da informação, sendo eles (Abreu, 2011):

- **Confidencialidade**: Visa garantir que apenas as pessoas autorizadas tenham acesso à informação.
- **Integridade**: Visa garantir que a informação se mantenha de forma íntegra, sem ser modificada ou perdida por qualquer evento não autorizado.
- **Disponibilidade**: Visa garantir que a informação esteja disponível sempre que necessário.

Figura 1 – Tríade da segurança da informação

Fonte: Abreu (2011).

Existem grandes desafios a serem encarados para garantir a segurança da informação nos dispositivos IoT, principalmente relacionado à baixa disponibilidade de recursos computacionais para se implementar medidas de segurança essenciais. Além disso, não existe um padrão de protocolo de segurança entre equipamentos, tornando-os muito mais suscetíveis a vários tipos de ataques. Também não é fácil detectar um equipamento infectado, visto que as redes não possuem capacidade de detecção de dispositivos IoT conectados a elas, e nem dos equipamentos que estão se comunicando entre si. (Everest Ridge, 2020).

Dentre os desafios mais comuns, podemos listar (Gerber; Kansal, 2020):

- **Proteger dispositivos restritos**: Dispositivos restritos necessitam de alto nível de criptografia, algo inviável para a baixa quantidade de recursos dos equipamentos.
- **Autorizar e autenticar dispositivos**: Devido à grande demanda de requisições em dispositivos IoT, é importante que utilizem níveis de autenticação fortes para não comprometer a segurança do sistema.
- **Proteger a comunicação**: Devido ao grande fluxo de troca de informações entre dispositivos, é importante garantir que essa informação esteja sendo transmitida de forma segura.
- **Garantir privacidade e integridade**: É necessário garantir que dados sensíveis sejam devidamente tratados e armazenados de maneira segura, além de garantir que o conteúdo dos dados permaneça intacto após transferidos entre os equipamentos.
- **Garantir alta disponibilidade**: Cada vez mais a sociedade se torna dependente do uso de redes e equipamentos IoT, tornando essencial que estejam protegidos contra falhas e ataques do tipo *Denial Of Service (*DoS), o qual se perde o acesso ao recurso devido a sua indisponibilidade.
- **Detecção de vulnerabilidades**: Devido à complexidade dos sistemas IoT, é necessário que sejam detectadas e tratadas vulnerabilidades nos equipamentos, a fim de evitar infecção de *softwares* maliciosos. O uso de inteligência artificial voltado para segurança da informação vem sendo uma prática bastante utilizada não apenas para detectar, mas para prever vulnerabilidades em dispositivos.

Ainda existem vários desafios a serem superados para garantir a segurança da informação em sistemas IoT, e isso vem sendo uma preocupação ainda maior no Brasil por conta da LGPD.

O uso de dispositivos IoT com *firmware* ou *software* atualizados, instalados em redes com múltiplas camadas de defesa com *firewall* e redes segregadas, aliada à adoção de plataformas com políticas de senha com autenticação de dois fatores, que transmitam dados criptografados e com redundância constituem medidas para mitigação dos problemas de segurança. A adoção de uma abordagem de segurança de informação – por padrão em todas as etapas de um projeto de dispositivos, aplicativos e serviços de IoT – assegura a privacidade e a integridade dos dados enquanto fornece dados, aplicativos e serviços IoT altamente disponíveis (Gerber; Kansal, 2020).

2.2 Internet das Coisas (IoT)

A Revolução Industrial é um grande marco na história da humanidade, pois mudou o processo produtivo de manufaturados para maquinofaturados, permitindo assim a criação de mais produtos no mercado e a preços menores. A revolução ocasionou um maior poder de compra e melhoria na qualidade de vida da população (Cavalcante; Silva, 2011). A primeira revolução industrial ocorreu entre os séculos XVIII a XIX com a introdução das máquinas a vapor, a segunda revolução com a chegada de energia elétrica no século XIX e início do século XX. Já a terceira revolução aconteceu devido ao grande desenvolvimento de semicondutores, *mainframes*, dos primeiros computadores e indícios da internet por volta dos anos de 1960 (Cavalcante; Silva, 2011).

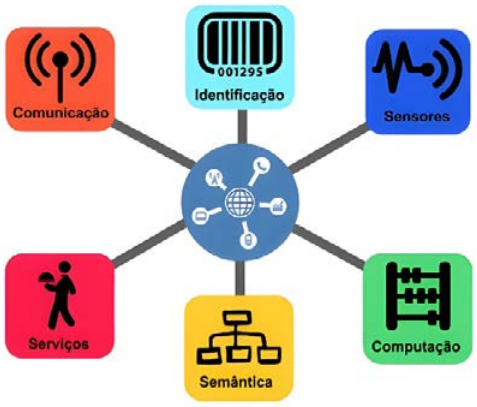
A quarta revolução industrial, também conhecida como Indústria 4.0, concentra-se na transformação digital, incluindo o desenvolvimento de automação, sistema inteligente, digitalização, análise de *big data*, IoT e inteligência artificial. A Indústria 4.0 é apresentada como o conceito de processo de manufatura baseado em tecnologia, integrado com tecnologias de informação e comunicação (Kagermann *et al*., 2013).

A integração de diversas tecnologias possibilita iniciativas como a do Centro de Operações Rio (COR), do município do Rio de Janeiro, que utiliza câmeras, radar meteorológico, GPS instalados em ônibus e diversos outros sensores para a coleta de dados sobre trânsito, chuvas e ocorrências diversas. As informações são combinadas e disponibilizadas para funcionários da Defesa Civil, iluminação e limpeza urbana, turismo etc., possibilitando

um empenho integrado na solução de problemas urbanos (Hojda; Martins; Fariniuk, 2020). Este cenário, que até poucos anos era ficção científica, requer múltiplos dispositivos, como veículos, câmeras, sensores etc. conectados à internet, de 8 bilhões em 2019, para 41 bilhões em 2027, de acordo com projeções (Newman, 2020).

Existem diversas classes de serviços que a IoT é capaz de prover, dentre elas, destacam-se os serviços de identificação, responsáveis por mapear entidades físicas em entidades virtuais, como, por exemplo a temperatura, uma entidade física, em seu valor em graus Celsius, uma entidade virtual (Santos *et al*., 2016)

Figura 2 – Blocos Básicos da IoT



Fonte: SANTOS *et al*., (2016).

Os dispositivos restritos são dispositivos cujas características são limitadas por razões de custo e/ou físicas. Dentre os limites existentes, um dispositivo restrito pode ter limites na capacidade de processamento, memória, consumo de energia elétrica e interface de utilização. Estas limitações podem ocorrer individualmente ou concomitantemente (Bormann *et al.,* 2014)

Os dispositivos restritos podem ser categorizados com Classe 0, 1 e 2, de acordo com sua capacidade de memória RAM e memória de armazenamento. Dispositivos Classe 0 são usados como sensores e normalmente não possuem capacidade de processamento para se comunicar através da internet de maneira segura. Dispositivos Classe 1 são capazes de implementar protocolos leves específicos para aplicações restritas e se comunicar de maneira segura através de redes IP. Por fim, os dispositivos Classe 2 possuem ainda menos restrições e suportam a maioria dos protocolos utilizados por computadores, embora a utilização de protocolos mais leves por consumirem menos energia e utilizarem menor banda de rede (Bormann *et al*., 2014). A Tabela 1 a seguir relaciona as classes com alguns exemplos de protocolos e camadas de rede.

Tabela 1 – Estrutura IoT

CAMADA	TECNOLOGIA OU PROTOCOLO	CLASSE DO DISPOSITIVO
Aplicação	CoAP,MQTT,AMQP,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: Oliveira *et al.,* (2019).

As limitações dos dispositivos restritos representam um grande desafio para a segurança da informação, pois muitos destes não são capazes de realizar criptografia e descriptografia complexa de modo rápido o suficiente para poder transmitir dados com segurança em tempo real e, muitas vezes, são vulneráveis a ataques de canal lateral (Gerber; Kansal, 2020). No entanto, devido à sua força de lei, a LGPD exige esses recursos aos projetos por meio de seu viés regulatório, embora isso não altere o fato de ainda ser um desafio no desenvolvimento de soluções de IoT.

3 Lei Geral de Proteção de Dados, Segurança de Informação e o IoT

3.1 Ataques a Dispositivos IoT na Atualidade

A Lei Federal no. 13.709, Lei Geral de Proteção de Dados ou LGPD, de 14 de agosto de 2018, é a principal regulamentação do Brasil destinada à proteção de dados pessoais. O *caput* do seu art. 1º discorre sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. Ainda neste ponto, as regras definidas na LGPD incluem também as fundações, as sociedades de economia mista e as empresas públicas (Brasil, 2018), estabelecidas ou não no Brasil, que processam dados pessoais para prestar bens ou serviços ao povo brasileiro (Amazon Web Services, s.d.)

Os dispositivos de automação residencial EA-1 e EA-3, da Control4 – cujos produtos estão disponíveis em mais de 100 países em 47.5000 lares, orquestrando mais de 15 milhões de dispositivos conectados (Control4, s.d) – possuem uma funcionalidade de recuperação de log que, em algumas versões do *firmware*, possui uma vulnerabilidade. Essa falha permite que um invasor execute o código como usuário root no sistema operacional (Tameesh, 2021), comprometendo a privacidade dos residentes, facilitando o roubo de informações pessoais ou confidenciais, o controle da automação residencial e até mesmo o monitoramento dos residentes dentro do ambiente de uma casa inteligente (Ali; Awad, 2018).

A BTicino é uma empresa presente em 180 países, atuando no desenvolvimento e fabricação dos produtos eletrônicos para automação residencial e objetos conectados da linha MyHome (BTicino, 2017). O produto BTI-454 é um servidor de áudio e vídeo que, em algumas versões do *firmware*, possui uma vulnerabilidade que permite que invasores não autenticados obtenham informações confidenciais do dispositivo, o que pode facilitar o comprometimento total do sistema (Securiteam, s.d.).

A Tuya Smart é uma plataforma global de desenvolvimento IoT que processa 122 milhões de interações de voz, por dia, através de 410.000 dispositivos ativos disponíveis em mais de 220 países (Tuya, s.d). Algumas das marcas cujos produtos utilizam a plataforma Tuya não implementam nenhum tipo de criptografia dos dados, deixando expostas informações como a senha da rede sem fio e até mesmo a chave RSA privada utilizada para se conectar aos servidores do fabricante (Coldewey, 2019).

Este tipo de negligência ilustra a falta de abordagem de segurança de informação por padrão que poderia ser evitada, ou ter os seus efeitos minimizados, através da adoção das seguintes práticas:

- Abordagem de segurança de informação por padrão durante as etapas de desenvolvimento, e após, de projetos de IoT (Gerber; Kansal, 2020);
- Formulação de boas práticas e regras de governança para o estabelecimento de condições organizacionais;
- Utilização de *gateways* para integrar a comunicação entre os dispositivos restritos de múltiplas classes e possibilitar comunicação segura através de redes IP (Jin *et al*., 2020);
- Rede de dispositivos IoT isolada dos outros dispositivos de rede (FBI, 2019);
- Uso de algoritmos criptográficos leves, como CLEFIA, para cifrar dados armazenados no dispositivo (Thakor; Razzaque; Khandaker, 2021).

Os desafios de segurança para dispositivos de IoT são muitos e envolvem desde o desenvolvimento das plataformas utilizadas por estes até os equipamentos físicos instalados. Os esforços dos fabricantes e desenvolvedores de dispositivos IoT na busca pela conformidade à Lei Geral de Proteção de Dados são de grande importância. Além do objetivo da proteção dos direitos fundamentais de liberdade e de privacidade dos dados pessoais, a aderência à LGPD pode evitar, ou atenuar, as sanções previstas em seu art. 52, sanções estas que variam entre uma advertência, multa, publicização da infração etc., até a proibição total do exercício de atividades relacionadas aos dados.

Os dispositivos de IoT facilitam a captação de informações sobre seus usuários. Os dados coletados podem ser utilizados para inferir padrões de comportamento e de uso dos recursos possibilitados pelo IoT. A LGPD é o expediente encontrado para determinação de conformidade no Brasil para coleta, transmissão e armazenamento de dados pessoais. Nessas circunstâncias, esforços precisam ser despendidos no apoio aos objetivos do LGPD através dos conceitos de segurança de informação (Oliveira *et al.,* 2019).

3.2 Coleta

Antes de iniciar qualquer tipo de tratamento de dados pessoais, deve-se disponibilizar meios que indiquem que a finalidade da operação seja registrada de forma clara e que os propósitos sejam informados ao titular. Caso não haja transparência para o utilizador, fica a pessoa jurídica de direito público ou privado sujeita às sanções administrativas descritas no capítulo 8 da referida Lei (Brasil, 2018).

A lei é aplicada à coleta e tratamento de dados, com objetivo de ofertar bens ou serviços em dados de indivíduos – que se encontrem em território nacional no momento da coleta – e deve ser feita com o consentimento expresso do titular a quem os dados se referem, com informações transparentes sobre o armazenamento, o uso e a proteção dos dados pessoais (Brasil, 2018). 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 do titular dos dados.

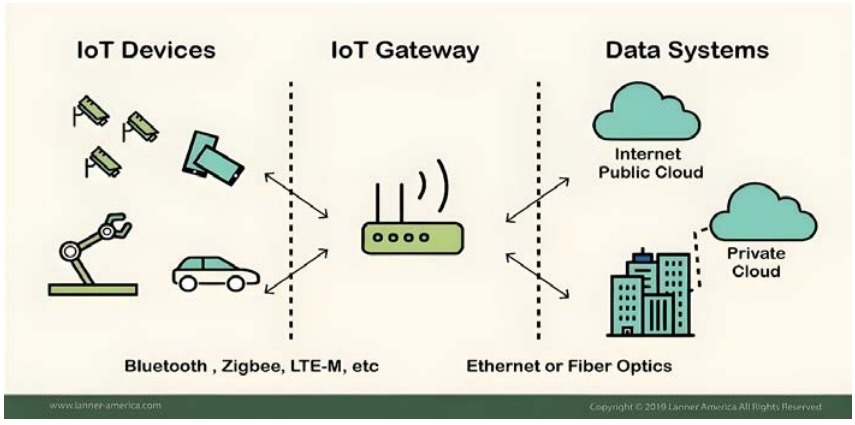
A LGPD, em seu art. 50, garante que os controladores e operadores dos dados coletados – no âmbito das suas competências, através de particulares ou associações – possam formular boas práticas e regras de governança para o estabelecimento de condições organizacionais visando a aderência à LGPD. Para além disso, a norma ABNT NBR ISO/IEC 27002 (2013), fornece diretrizes para procedimentos de gestão de segurança da informação e normas de segurança da informação que podem ser aplicadas a fim de obter-se estas práticas.

3.3 Transmissão

O grande desafio para a transmissão segura de dados se dá por conta dos dispositivos restritos da Classe 0, normalmente utilizados como sensores que coletam entidades físicas e as transmitem utilizando tecnologias sem fio, com baixo consumo elétrico e baixas taxas de transmissão, e que não possuem capacidade de processamento para uma comunicação segura via internet (Oliveira *et al.,* 2019).

A utilização de *gateways* possibilita localmente o processamento de informações na rede dos dispositivos IoT, de maneira central, com potencial para mitigar problemas de privacidade e de restrições de rede em cenários heterogêneos, onde podem coexistir dispositivos IoT com diferentes tipos de recursos e restrições, (Jin *et al*., 2020).

Figura 3 – IoT Gateway



Fonte: Lanner, 2019.

Usar redes separadas para isolar os dispositivos IoT dos outros dispositivos de rede, como servidores de computadores, também ajuda a estabelecer uma comunicação privada e segura de dados confidenciais (FBI, 2019). Outras medidas incluem o uso de *firewalls*, restrição do acesso físico aos dispositivos de rede, utilização de senhas de uso único geradas aleatoriamente e desativação de funções do sistema operacional que não são exigidas pelo dispositivo (Gerber; Kansal, 2020).

3.4 Armazenamento

Os dispositivos restritos, frequentemente, precisam ser capazes de funcionar com pouca energia, por exemplo, quando usam baterias. Os dados armazenados podem ser criptografados, especialmente informações

de dados confidenciais e/ou sensíveis. No entanto, os dispositivos restritos podem não ser capazes de realizar operações de criptografia e descriptografia em tempo real (Gerber; Kansal, 2020).

Do ponto de vista de segurança da informação, a indisponibilidade imediata dos dados afetará, por exemplo, os controles que visam prevenir vazamento de dados (Oliveira *et al.,* 2019), o que consequentemente também afetará na adequação do LGPD. Desse modo, especifica-se a confirmação de existência ou o acesso a dados pessoais, que deve ocorrer de maneira imediata (Brasil, 2018).

Além disso, a falta da disponibilização imediata pode afetar, por exemplo, as medidas de controle criadas para evitar esse vazamento de dados, proteger a borda da rede e outras etapas do ciclo de vida das informações (Oliveira *et al.,* 2019). Portanto, em razão dos altos requisitos para implementar criptografia tradicional, como AES, RSA, SHA-3, em dispositivos IoT restritos (Tachibana, 2017), o uso de algoritmos criptográficos leves torna-se uma opção viável.

O uso de algoritmos criptográficos leves – como o CLEFIA, PRESENT, SIMON e SPECK – constitui uma maneira efetiva de dar segurança aos dados com custo e performance aceitáveis para dispositivos restritos (Thakor; Razzaque; Khandaker, 2021). Embora com menores níveis de segurança que algoritmos de criptografia tradicional, o uso de cifras leves como alternativa ao armazenamento em texto claro traz benefícios significativos à privacidade dos dados.

3.5 Desafios da Segurança da Informação em IoT sob o Prisma da LGPD

A segurança em sistemas IoT confronta limitações intrínsecas de dispositivos restritos (processamento, memória, energia), que representam um desafio à implementação de criptografia robusta. Sensores Classe 0, comuns em casas inteligentes, não são capazes de executarem algoritmos como AES/RSA (Gerber; Kansal, 2020), divergindo do Art. 46 da LGPD, que exigem proteção contra acessos não autorizados.

Casos como as vulnerabilidades em dispositivos Control4, onde falhas no *firmware* permitiam acesso remoto a dados sensíveis (Tameesh, 2021), ilustram o conflito entre conformidade legal e restrições técnicas. Enquanto a LGPD prevê multas de 2% do faturamento por violações (Art. 52), dispositivos de baixo custo ainda armazenam senhas em texto claro ou usam chaves RSA estáticas (Coldewey, 2019).

Na transmissão, redes heterogêneas exigem *gateways* para intermediar comunicações seguras (Jin *et al*., 2020), alinhando-se ao Art. 6º da LGPD sobre transparência. Redes isoladas para IoT são eficazes, mas sua implementação pode varia em custo e complexidade, a depender do ambiente de uso (residencial ou corporativo) (FBI, 2019).

No armazenamento, cifras leves (CLEFIA, PRESENT) equilibram desempenho e conformidade, embora ofereçam segurança inferior à criptografia tradicional (Thakor; Razzaque; Khandaker, 2021). Isso levanta um dilema: soluções viáveis atendem ao princípio de “proteção desde a concepção” (Art. 46, LGPD)? A resposta demanda integração entre normas (ISO 27002) e inovação em segurança cibernética adaptada à IoT.

4 Conclusão

A IoT será transformadora para todos os tipos de organizações, com expectativa de grande crescimento do mercado. As aplicações são variadas e oferecem muitos benefícios como conforto, segurança e aumento de produtividade para indivíduos e organizações que utilizam esta tecnologia. Os dispositivos de IoT podem coletar uma vasta quantidade de dados e possibilitam grande compreensão do comportamento dos seus usuários. O uso das informações coletadas para o oferecimento de produtos e serviços sob medida ameaça a privacidade dos indivíduos que são constantemente vigiados.

A Lei Geral de Proteção de Dados, ou LGPD, em vigor desde 14 de agosto de 2018, amplificou a preocupação com a confidencialidade, integridade e disponibilidade dos dados, aumentando a importância da aplicação de soluções que tenham em mente as limitações de armazenamento, memória e capacidade de processamento dos dispositivos IoT restritos.

A existência de vulnerabilidades em alguns produtos e serviços de grandes fornecedores de produtos e serviços de IoT – como Control4, BTicino e Tuya, que juntas orquestram milhões de dispositivos conectados em milhares de lares espalhados em centenas de países – evidenciam a importância da busca pela conformidade

com a LGPD, tanto do ponto de vista da proteção dos dados, quanto para prevenir ou atenuar sanções previstas pela lei.

Em virtude dos desafios ocasionados pelos dispositivos restritos e a necessidade do atingimento dos requisitos legais da LGPD, foram abordadas soluções identificadas na literatura existente relacionadas à aplicação e impacto dos mecanismos e tecnologias referentes à coleta, transmissão e armazenamento dos dados.

Embora o presente trabalho contribua para o entendimento dos desafios regulatórios impostos pela LGPD no contexto da IoT, algumas limitações devem ser levadas em consideração. A investigação, portanto, baseou-se essencialmente em revisão de literatura, sem incluir validações empíricas ou estudos concretos de caso. Ressalta-se, por fim, que as soluções sugeridas, embora alinhadas à bibliografia especializada, não foram submetidas à análise de viabilidade técnica, econômica ou jurídica no contexto da LGPD.

Dentre as possibilidades para pesquisas futuras, destaca-se a análise da viabilidade técnica da utilização de criptografias tradicionais, como AES, RSA e SHA-3, em dispositivos de IoT. Também se sugere o desenvolvimento de guias orientativos voltados ao desenvolvimento e implementação de soluções seguras no contexto de IoT. Por fim, a adoção de tecnologias baseadas em *blockchain* para reforçar a segurança, por meio de registros imutáveis e autenticação descentralizada.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**: tecnologia da informação — técnicas de segurança — código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013. Disponível em: https://manuais.satc.edu.br/lib/exe/fetch.php?media=iso:iso_iec_27002.pdf. Acesso em: 18 abr. 2024.

ABREU, L. F. dos S. **A segurança da informação nas redes sociais**. 2011. Monografia (Curso Técnico em Processamento de Dados) – Faculdade de Tecnologia de São Paulo, São Paulo, 2011. Disponível em: https://www.fatecsp.br/dti/tcc/tcc0023.pdf. Acesso em: 10 ago. 2021.

AFFONSO, E. P. **A insciência do usuário na fase de coleta de dados**: privacidade em foco. 2018. Tese (Doutorado em Ciência da Informação) – Faculdade de Filosofia e Ciência, Universidade Estadual Paulista, Marília, São Paulo, 2018. Disponível em: https://www.marilia.unesp.br/Home/Pos-Graduacao/CienciadaInformacao/Dissertacoes/affonso_ep_do_mar.pdf. Acesso em: 6 ago. 2021.

ALI, B.; AWAD, A. W. Cyber and physical security vulnerability assessment for IoT-based smart homes. **Sensors**, [*s. l.*], v. 18, n. 3, p. 1-17, 2018. Disponível em: https://www.mdpi.com/1424-8220/18/3/817/htm. Acesso em: 3 ago. 2021.

AMAZON WEB SERVICES. Privacidade de dados no Brasil. [*S.l.*], 2024. Disponível em: https://aws.amazon.com/pt/compliance/brazil-data-privacy/. Acesso em: 7 ago. 2021.

BORMANN, C.; ERSUE, M.; KERANEN, *A. Terminology for Constrained-Node Networks*. 2014. Disponível em: https://datatracker.ietf.org/doc/html/rfc7228. Acesso em: 14 de ago. 2021.

BTCINO**.** BTicino company profile*.* [S.l.: s.n.], 2018. Disponível em: https://www.bticino.com/media/2018/10/2018-BT-ISTITUZIONALE_EN.pdf. Acesso em: 3 set. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 abr. 2024.

CAVALCANTE, Z. V.; SILVA, M. L. S. da. A importância da Revolução Industrial no mundo da tecnologia. *In:* ENCONTRO INTERNACIONAL DE PRODUÇÃO CIENTÍFICA, 7., 2011, Maringá. **Anais** [...]. Maringá: Cesumar, 2011. p. 1-6. Disponível em: https://www.unicesumar.edu.br/epcc-2011/wp-content/uploads/sites/86/2016/07/zedequias_vieira_cavalcante2.pdf. Acesso em: 11 ago. 2021.

COLDEWEY, Devin. Cheap Internet of Things gadgets betray you — even after you toss them in the trash. TechCrunch, 30 jan. 2019. Disponível em: https://techcrunch.com/2019/01/30/cheap-internet-of-things-gadgets-betray-you-even-after-you-toss-them-in-the-trash/. Acesso em: 18 ago. 2021.

CONTROL4. About Control4. [S.l.: s.n.], [s.d.]. Disponível em: https://www.control4.com/company. Acesso em: 1 set. 2021.

EVEREST RIDGE. Segurança da informação para IoT. Everest Ridge, 2020. Disponível em: https://everestridge.com.br/seguranca-da-informacao-para-iot/. Acesso em: 11 ago. 2021.

FBI. Tech Tuesday: Internet of Things (IoT). [S.l.: s.n.], 2019. Disponível em: https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot. Acesso em: 11 ago. 2021.

GERBER, Anna; KANSAL, Satwik. Os 10 maiores desafios de segurança em IoT. [*S.l.: s.n.*], 2020. Disponível em: https://developer.ibm.com/br/articles/iot-lp201-iot-architectures/. Acesso em: 7 ago. 2021.

HOJDA, A.; MARTINS, P.; FARINIUK, T. M. D. Da cidade inteligente à inteligência nas operações urbanas: o caso do Centro de Operações Rio. **Revista Líder**, [*s. l.*], v. 36, n. 22, p. 104–131, 2020. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8004680. Acesso em: 2 set. 2021.

JIN, W.; XU, R.; YOU, T.; HONG, Y.-G.; KIM, D. Secure edge computing management based on independent microservices providers for gateway-centric IoT networks. **IEEE Access**, [*s. l.*], v. 8, p. 187975–187990, 2020. DOI: https://doi.org/10.1109/ACCESS.2020.3030297

KAGERMANN, H.; WAHLSTER, W.; HELBIG, J. Recommendations for implementing the strategic initiative Industrie 4.0: final report of the Industrie 4.0 Working Group. *Frankfurt: Acatech – National Academy of Science and Engineering*, 2013. Disponível em: https://en.acatech.de/publication/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/. Acesso em: 29 abr. 2024.

LANNER ELECTRONICS INC. What is an IoT Gateway? Lanner Electronics Blog, [s.d.]. Disponível em: https://www.lanner-america.com/blog/what-is-an-iot-gateway/. Acesso em: 14 ago. 2021.

LIN, J.; YU, W.; ZHANG, N.; YANG, X.; ZHANG, H.; ZHAO, W. A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications. **Renewable and Sustainable Energy Reviews**, [*s. l.*], v. 4, n. 5, p. 1125-1142, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S1364032120305128. Acesso em: 18 abr. 2024.

LIU, J.; ZHANG, C.; FANG, Y. EPIC: a differential privacy framework to defend smart homes against internet traffic analysis. **IEEE Internet of Things Journal**, [*s. l.*], v. 5, n. 2, p. 1206–1217, abr. 2018. DOI: https://doi.org/10.1109/JIOT.2018.2799820

MAGALHÃES, R.; VENDRAMINI, A. Os impactos da quarta revolução industrial. **Gv-Executivo**, [*s. l.*], v. 17, n. 1, p. 40–43, 2018. DOI: https://doi.org/10.12660/gvexec.v17n1.2018.74093

NEWMAN, P. The Internet of Things 2020. **Business Insider**, 6 mar. 2020. Tech. Disponível em: https://www.businessinsider.com/internet-of-things-report. Acesso em: 29 abr. 2024.

OLIVEIRA, D. B. de; VEGA, G. C. M. A proteção da privacidade pela lei geral de proteção de dados (LGPD) na era da internet das coisas (IOT). **Revista de Direito**, [*s. l.*], v. 16, n. 02, p. 01–30, 2024. DOI: https://doi.org/10.32361/2024160219351.

OLIVEIRA, N. S. de; GOMES, M. A.; LOPES, R.; NOBRE, J. C. Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). **Revista Eletrônica de Iniciação Científica em Computação,** [*s. l.*], v. 17, n. 4, p. 1-14, 2019. Disponível em: https://seer.ufrgs.br/reic/article/download/88790/55009. Acesso em: 3 de ago. 2021.

RODRIGUES NETO, E. de C. **Estudo sobre aplicações de IoT na área médica**. 2020. Trabalho de Conclusão de Curso (Graduação em Engenharia Eletrônica) – Departamento de Engenharia Eletrica e Eletrônica, Universidade Federal de Santa Catarina, Florianópolis, Santa Catarina, 2020. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/204169/TCC_Ebert_Final.pdf. Acesso em: 7 ago. 2021.

SANTOS, Bruno; SILVA, Lucas; CELES, Clayson; NETO, João; PERES, Bruna; VIEIRA, Marcos; VIEIRA, Luiz; GOUSSEVSKAIA, Olga; LOUREIRO, Antonio. 2016. *Internet das coisas: da teoria à prática*. Disponível em: https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf. Acesso em: 3 de ago. 2021.

SECURITEAM. Legrand and Bticino Information Disclosure Vulnerability. [s.d.]. Disponível em: https://securiteam.com/securitynews/6l03j1f5py/. Acesso em: 3 set. 2021.

TACHIBANA, F. M. O. **Implementação em hardware e sistemas embarcados de algoritmos de criptografia leve para aplicação em IoT**. 2017. Monografia (Graduação em Ciência da Computação) – Centro Universitário Eurípides, Marília, São Paulo, 2017. Disponível em: https://aberto.univem.edu.br/handle/11077/1649. Acesso em: 16 de ago. 2021.

TAMEESH, F. Cyber secure select: protecting high-net-worth individuals. **Aon Cyber Solutions**, 28 jun. 2021. Disponível em: https://www.aon.com/cyber-solutions/aon_cyber_labs/cyber-secure-select-protecting-high-net-worth-individuals/. Acesso em: 3 set. 2021.

THAKOR, V. A.; RAZZAQUE, M. A.; KHANDAKER, M. R. A. Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities. **IEEE Access**, [*s. l.*], v. 9, p. 28177–28193, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3052867

TUYA. Global AIoT Development Platform. [*S.l.: s.n.*], [s.d.]. Disponível em: https://www.tuya.com/about. Acesso em: 18 ago. 2021.

WACHTER, S. W. Normative challenges of identification in the Internet of Things: privacy, profiling, discrimination, and the GDPR. **Computer Law & Security Review**, [*s. l.*], v. 34, n. 3, p. 436–449, 2018. DOI: https://doi.org/10.1016/j.clsr.2018.02.002

ZINS, C. Conceptual approaches for defining data, information, and knowledge. **Journal of the American Society for Information Science and Technology**, [*s. l.*], v. 58, n. 4, p. 479–493, 2007. DOI: https://doi.org/10.1002/asi.20508

Sobre os Autores

Antonio Alisio de Meneses Cordeiro
Graduado em Engenharia Eletrônica pela Universidade de Fortaleza (2004), com MBA em Redes de Sistemas e Telecomunicações pela Universidade de Fortaleza (2021) e especialização em Ciência de Dados pela Universidade Federal do Rio Grande do Sul (2025). Tem experiência em microeletrônica, sistemas de telecomunicações, administração de servidores Linux. Atualmente é cientista de dados no Serviço Federal de Processamento de Dados, atuando no desenvolvimento de soluções em inteligência. Trabalha com integração de Grandes Modelos de Linguagem (LLMs) em fluxos institucionais e práticas de LLMOps. Também atua como artista independente nas áreas de música e trilha sonora para jogos.

Leandro Lima Sobral
Graduado em Engenharia de Telecomunicações pela Universidade de Fortaleza - UNIFOR (2019). Atualmente é aluno do MBA Redes e Telecom. Tem experiência em telecomunicações e Governança e Gerenciamento de Serviços de TI. Analista sênior na G4Flex Business & Services.

Como citar:

CORDEIRO, Antonio Alísio de Meneses; Sobral, Leandro Lima. Desafios Regulatórios da Lei Geral de Proteção de Dados (LGPD) para Internet das Coisas (IoT). **Rev. Tecnol.**, Fortaleza, v. 45, p. 1-11, 2024. DOI: https://doi.org/10.5020/23180730.2024.13998

Aceito em: 27/03/2023
Avaliado em: 20/05/2024