



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS PICOS
CURSO TECNÓLOGO EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

MARIA EDUARDA FERREIRA OLIVEIRA

**PRIVACIDADE NA INTERNET DAS COISAS: uma análise crítica dos
desafios de segurança no contexto da LGPD**

PICOS
2026

MARIA EDUARDA FERREIRA OLIVEIRA

PRIVACIDADE NA INTERNET DAS COISAS: uma análise crítica dos desafios
de segurança no contexto da LGPD

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso Tecnólogo em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Picos.

Orientador: Prof. Mestre Ciro Ferreira de Carvalho Júnior.

AGRADECIMENTOS

Este momento tem sido marcado por grandes emoções e profunda alegria, mas, acima de tudo, por muita oração e fé. Por isso, escreverei estes agradecimentos com muito amor.

Deus me concedeu força para trilhar esse caminho e concluir essa etapa. Sem Sua luz, nada disso seria possível. Ao meu lado, junto d'Ele, estive também Nossa Senhora, que sempre me cobriu com seu manto de amor, enxugou minhas lágrimas quando necessário e sorriu comigo nos momentos felizes. Então, de modo especial, eu, Maria Eduarda, agradeço a Deus e a Nossa Senhora, pois sem suas misericórdias e sustento, eu jamais chegaria até aqui. Acredito fielmente que os terços rezados aos domingos na Igreja Catedral foram atendidos.

Ao meu pai, Valdinar, que tem mãos calejadas, pele queimada do sol e que tanto me ensina sobre honestidade, amor ao próximo e respeito, amo você muito mais do que palavras podem expressar.

À minha mãe, Luiza, dona deste Artigo, minha amiga, meu Norte e meu exemplo de fé em Deus, eu nunca encontrei um trevo de quatro folhas, mas cresci ouvindo: "queria ter uma mãe como a sua". Com o tempo, percebi que a sorte vem de maneiras diferentes para cada pessoa, e a minha sempre foi ter você. Suas orações são o meu escudo, e sei que fui muito abençoada por Deus e Nossa Senhora por colocar uma mulher assim em minha vida.

Esse trabalho é mais de vocês do que meu, pois eu escrevi as palavras neste documento, mas foram vocês que tornaram tudo isso possível. Sei que posso voar alto e tenho a certeza de que tenho uma casa para voltar. Nós conseguimos: a filha de vocês está formada.

Ao meu irmão, Paulo, e aos meus primos, quero dizer que cada brincadeira, palavra de apoio, crise de riso e férias na serra me mostraram que a vida só é pesada quando não se tem a leveza que vocês carregam. Não existe a menor possibilidade de alguém me conhecer e não saber quem são vocês, pois são uma parte essencial de quem eu sou. O amor que sinto por cada um não seria possível descrever nem em cem páginas.

Aos meus avós, tios, tias, padrinhos e madrinhas, que em momento algum duvidaram do meu potencial, obrigada pelo incentivo, por comemorarem cada conquista minha e por me apoiarem. Sei que tenho muitos pais e muitas mães que

moveriam montanhas para me ver segura e feliz. A cada dia que passa, percebo ainda mais o quanto é valioso ter cada um em minha vida.

Aos meus amigos e colegas, cada momento de descontração foi alívio nos dias mais pesados. Obrigada por me escutarem, por entenderem que minha ausência nunca foi por falta de amor, e, acima de tudo, obrigada por enxergarem em mim uma mulher tão grande e forte.

À minha prima Amanda e à minha amiga Ana, que estiveram comigo em sala de aula, quero dizer que foi uma dádiva viver esta etapa ao lado de vocês, um prazer imenso ser uma das “*Meninas Super Poderosas*” do campus. Obrigada por serem colo e confiança em cada dia desse processo. Guardarei com amor nossos slides de seminários temáticos e sentirei falta dos nossos lanches.

Ao meu orientador e demais professores, que foram pilares importantes na minha jornada, deixo também meu reconhecimento e gratidão. Cada ensinamento que recebi em sala de aula é agora parte de quem sou.

E, a você que está lendo, afirmo que a parte mais difícil de um TCC não é escrever o Artigo, mas agradecer sem derramar rios de lágrimas por todos aqueles que fizeram isso possível.

PRIVACIDADE NA INTERNET DAS COISAS: uma análise crítica dos desafios de segurança no contexto da LGPD

Maria Eduarda Ferreira Oliveira¹
Ciro Ferreira de Carvalho Júnior²

RESUMO

O avanço da Internet das Coisas (IoT) tem ampliado a conectividade entre dispositivos e a coleta de dados pessoais, trazendo desafios relacionados à segurança e à proteção da privacidade dos usuários. Nesse contexto, este estudo tem como objetivo analisar de que forma as limitações técnicas dos dispositivos IoT influenciam a adequação às diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD). A pesquisa caracteriza-se como exploratória, descritiva, de abordagem qualitativa e desenvolvida por meio de revisão sistematizada da literatura. Os resultados mostram que as limitações de processamento, memória e consumo de energia dificultam a implementação de mecanismos de segurança compatíveis com as exigências da legislação. Também evidenciam que soluções como protocolos leves de comunicação, criptografia leve e gateways de segurança contribuem para reduzir essas limitações, fortalecendo a proteção dos dados pessoais e favorecendo a conformidade com a LGPD. Conclui-se que a proteção da privacidade em ambientes de Internet das Coisas depende tanto do atendimento aos requisitos legais quanto da adoção de soluções técnicas compatíveis com as restrições desses dispositivos.

Palavras-chave: internet das coisas; proteção de dados; lei geral de proteção de dados pessoais; privacidade; segurança.

ABSTRACT

The advancement of the Internet of Things (IoT) has expanded connectivity among devices and the collection of personal data, raising challenges related to security and the protection of user privacy. In this context, this study aims to analyze how the technical limitations of IoT devices influence compliance with the guidelines of the General Personal Data Protection Law (LGPD). The research is exploratory and descriptive in nature, employing a qualitative approach and conducted through a systematic literature review. The results show that limitations in processing power, memory, and energy consumption hinder the implementation of security mechanisms compatible with the requirements of the legislation. They also demonstrate that solutions such as lightweight communication protocols, lightweight encryption, and security gateways help reduce these limitations, strengthening the protection of personal data and promoting compliance with the LGPD. It is concluded that privacy protection in Internet of Things environments depends both on meeting legal requirements and on adopting technical solutions compatible with the constraints of these devices.

Keywords: internet of things; data protection; general personal data protection law; privacy; security.

Data de aprovação: 30/07/2026 (data de apresentação do TCC)

¹ Graduanda em Análise e Desenvolvimento de Sistemas. Instituto Federal do Piauí - Campus Picos. mariaolvr@gmail.com.

² Mestre em Sistemas e Computação. Professor EEBT no IFPI e Advogado. ciro.junior@ifpi.edu.br.

1 INTRODUÇÃO

O avanço da Internet das Coisas (*Internet of Things* – IoT) tem promovido transformações significativas na forma como pessoas e sistemas interagem no ambiente digital. Carvalho (2020) aponta que a incorporação desses dispositivos no cotidiano ampliou as possibilidades de automação, monitoramento e otimização de tempo em diferentes contextos, como residências, cidades, saúde e indústria.

No entanto, o crescimento contínuo da IoT intensificou a coleta e o tratamento de informações, tornando a privacidade uma preocupação cada vez mais relevante devido ao grande volume de dados pessoais e sensíveis envolvidos. Muitos dispositivos operam de forma contínua, coletando informações sem que os usuários tenham plena consciência desse processo ou controle efetivo sobre a forma como seus dados são tratados. Nesse contexto, garantir a privacidade em ambientes altamente conectados torna-se um desafio de segurança ainda maior do que aquele observado nas redes tradicionais (Bianchini; Silva; Dias, 2024)

Além dos benefícios proporcionados pela conectividade, a coleta indiscriminada de informações pode comprometer a autonomia dos usuários e ampliar riscos relacionados ao uso indevido de dados pessoais (Alves; Peixoto; Rosa, 2021).

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece princípios e diretrizes para o tratamento dessas informações, oferecendo mecanismos que contribuem para a proteção dos titulares de dados e para a promoção de práticas mais seguras em sistemas conectados (Alencar, 2023).

Diante disso, faz-se necessário entender de que forma as limitações técnicas dos dispositivos IoT afetam o cumprimento das diretrizes estabelecidas pela LGPD, em especial ao que tange a privacidade dos usuários.

O objetivo deste estudo consiste em analisar de que forma as limitações técnicas dos dispositivos IoT influenciam a adequação às exigências de proteção de dados previstas na LGPD, considerando seus impactos sobre a privacidade dos usuários e a segurança das informações em ambientes conectados.

Para alcançar esse objetivo, foram realizadas as seguintes etapas: i) realizar um levantamento bibliográfico e documental sobre a IoT, abordando seus conceitos, características e aspectos relacionados ao tratamento de dados pessoais; ii) analisar a relação entre os pilares da Segurança da Informação e as limitações técnicas dos

dispositivos IoT, com ênfase em aspectos como capacidade de processamento, armazenamento, consumo de energia e seus reflexos na proteção da privacidade; iii) examinar as exigências da LGPD aplicáveis ao contexto da IoT, buscando identificar possíveis incompatibilidades entre os requisitos legais de proteção de dados e as restrições técnicas presentes nesses dispositivos.

A relevância deste estudo está associada à crescente expansão da Internet das Coisas e aos impactos que essa tecnologia exerce sobre a privacidade dos usuários, especialmente em razão da coleta contínua e do tratamento de dados pessoais por dispositivos conectados. Do ponto de vista técnico, a pesquisa contribui para a compreensão de algumas restrições físicas, como processamento, bateria e armazenamento, inerentes aos sistemas IoT, bem como de seus reflexos na proteção das informações. Sob a perspectiva social, o estudo torna-se pertinente diante da ampla presença dessas tecnologias no cotidiano, favorecendo a discussão sobre os riscos à privacidade e a importância da adoção de práticas mais seguras e responsáveis no tratamento de dados.

Quanto aos procedimentos metodológicos, a pesquisa caracteriza-se como bibliográfica, de abordagem qualitativa e caráter exploratório-descritivo. O estudo foi desenvolvido por meio de uma revisão sistematizada da literatura, com o objetivo de reunir e analisar produções científicas relacionadas à IoT, segurança da informação e privacidade. A análise dos estudos selecionados buscou identificar padrões, conceitos recorrentes e contribuições teóricas que permitam compreender os principais desafios da privacidade em ambientes IoT e sua relação com as diretrizes estabelecidas pela LGPD.

Por fim, além desta introdução, o trabalho está organizado em seções que apresentam o referencial teórico sobre IoT privacidade e LGPD; os procedimentos metodológicos adotados; os resultados e a discussão obtidos a partir da análise da literatura; e, por fim, as considerações finais, que destacam as principais conclusões do estudo.

2 FUNDAMENTOS TÉCNICOS E NORMATIVOS DA PRIVACIDADE NA INTERNET DAS COISAS

2.1 INTERNET DAS COISAS

Considerada uma das principais transformações tecnológicas do século XXI, a IoT refere-se à conexão de objetos do cotidiano à *Internet*, permitindo que eles se comuniquem e interajam entre si. Esses dispositivos podem ser controlados remotamente e oferecem diversas funcionalidades, como a automação de tarefas, a coleta de dados e a otimização de atividades do dia a dia (Calaza, 2024).

A partir de 2010, houve um crescimento significativo do interesse científico pela IoT, contribuindo para sua consolidação como uma infraestrutura global dinâmica e interoperável. Nesse contexto, objetos físicos e virtuais passaram a possuir identidades próprias e a se integrar às redes de informação (Dachyar; Zagloel; Saragih, 2019).

Carvalho (2020) afirma que atualmente a IoT traz grandes facilidades para todos. Segundo o autor, já é possível observar casas equipadas com *Smart TVs*, termostatos, geladeiras e fechaduras inteligentes. Na área da saúde, a IoT traz benefícios ao integrar o prontuário do paciente, mostrando o seu estado clínico, por exemplo. Na agricultura, já se usam sensores para o monitoramento de aspectos como temperatura, umidade do solo e do ar.

2.1.1 ARQUITETURA DISPOSITIVOS IOT

Para viabilizar aplicações IoT, a literatura propõe modelos estruturados em camadas que organizam o fluxo da informação. Entre os mais utilizados, encontram-se a arquitetura de três camadas e a arquitetura de cinco camadas, conforme ilustrado na Figura 1 (Costa, 2022; Rodrigues, 2025).

Figura 1: Arquiteturas de 3 e 5 camadas.



Fonte: Elaborado pela autora (2025), adaptado de Costa (2022) e Rodrigues (2025).

O modelo de três camadas (física, rede e aplicação) é o mais adotado em abordagens iniciais por sintetizar o funcionamento básico do sistema. Nele, a camada física é a responsável pela coleta de dados do ambiente real (Costa, 2022). Entretanto, é nela que se concentram os maiores desafios de segurança, devido à capacidade computacional reduzida dos sensores, o que dificulta a implementação nativa de algoritmos de criptografia (Cordeiro; Sobral, 2024; Rodrigues, 2025).

Com o aumento da complexidade e das exigências de privacidade (como as previstas na LGPD), o modelo de cinco camadas torna-se mais adequado. Ele introduz a camada de processamento (ou *middleware*), que atua como um intermediário estratégico para filtrar e armazenar dados, permitindo a integração de mecanismos de segurança suplementares que o *hardware* básico não suporta. Por fim, a camada de negócio gerencia o ecossistema sob uma perspectiva estratégica, garantindo que o tratamento dos dados esteja alinhado aos objetivos e regras do sistema (Cordeiro; Sobral, 2024).

2.2 PILARES DA SEGURANÇA DA INFORMAÇÃO

Os pilares que estruturam a Segurança da Informação (SI) orientam todas as práticas de proteção de dados, classificando a SI como o conjunto de práticas voltadas à proteção de informações contra acessos, modificações ou destruições não autorizadas, visando preservar o valor dos ativos para instituições e indivíduos (IBM, 2024).

No contexto governamental e técnico, esse conjunto de práticas costumam se basear em quatro pilares: Confidencialidade, Integridade, Disponibilidade e Autenticidade (Brasil, 2024), sendo:

- **Confidencialidade:** informações pessoais e institucionais devem ser acessadas apenas por pessoas autorizadas;
- **Integridade:** os dados devem manter sua veracidade e consistência, sem modificações indevidas durante seu ciclo de vida;
- **Disponibilidade:** as informações devem estar acessíveis para quem precisa, no momento certo e conforme regras estabelecidas;
- **Autenticidade:** as informações devem ser associadas de forma confiável à pessoa, sistema ou entidade que as produziu ou modificou.

Apesar da aplicação desses pilares, sua aplicação prática na IoT é complexa, já que esses dispositivos lidam com grandes volumes de dados sensíveis (Fornasier, 2020).

Nesse contexto, a efetivação dos pilares da SI não depende apenas de *software*, mas também das capacidades técnicas dos dispositivos utilizados (Cordeiro; Sobral, 2024; Soares; Alencar, 2025).

Entretanto, a limitada capacidade de processamento e as restrições de memória e energia presentes em muitos dispositivos IoT representam obstáculos à implementação de mecanismos avançados de segurança, uma vez que podem afetar significativamente o desempenho destes dispositivos. Dessa forma, torna-se necessário adotar soluções que equilibrem proteção e desempenho, sem comprometer a disponibilidade e a integridade das operações (Rocha Neto *et al.*, 2025; Rodrigues, 2025).

2.3 PRIVACIDADE EM DISPOSITIVOS IOT

A discussão sobre privacidade torna-se relevante após a apresentação dos pilares da SI, pois o crescimento exponencial de objetos inteligentes, estimado em mais de 32 bilhões de conexões até 2030, amplia a superfície de exposição dos indivíduos (Rodrigues, 2025).

Diante desse contexto, é fundamental definir o que se entende por privacidade. Para Panek (2019), a privacidade constitui um princípio essencial para a proteção de dados, assegurando que as informações sejam controladas exclusivamente por seus respectivos usuários, que terceiros não tenham acesso ou autorização para processá-las e que o uso dos dados recebidos não permita a realização de inferências adicionais. Ou seja, trata-se de um princípio que protege a individualidade e garante que cada usuário mantenha controle sobre suas próprias informações.

Entretanto, na prática, muitos dispositivos conectados realizam a coleta de dados sem que os usuários compreendam plenamente as implicações desse processo (Siqueira *et al.*, 2021). Um exemplo são as Smart TVs. Ao concordar com os termos de uso e as políticas de privacidade dos fabricantes, os usuários podem autorizar a coleta de diferentes informações, como dados de localização, preferências de consumo, endereços IP, cookies e credenciais de autenticação, aumentando a exposição a riscos de privacidade e segurança (Alves; Peixoto; Rosa, 2021).

Esse cenário confronta diretamente a LGPD, que exige que o tratamento de dados pessoais ocorra mediante consentimento expresso e com transparência sobre o armazenamento e proteção (Cordeiro; Sobral, 2024; Costa, 2022).

2.4 LIMITAÇÕES TÉCNICAS NOS DISPOSITIVOS IOT

Diferente dos sistemas convencionais, a IoT é composta por dispositivos com recursos limitados, o que dificulta a implementação de medidas de segurança consideradas essenciais em outros ambientes computacionais. Essas limitações se manifestam principalmente em três pilares: capacidade de processamento, memória e consumo de energia (Cordeiro; Sobral, 2024; De Oliveira *et al.*, 2019).

As especificações de processamento impedem a adoção de algoritmos de segurança avançados e criptografia robusta (como RSA e AES), uma vez que o aparelho não consegue fazer cálculos complexos rápido o bastante para garantir a transmissão de dados em tempo real (Cordeiro; Sobral, 2024; Sousa; Silva, 2025). Consequentemente, se a informação não pode ser acessada imediatamente, as ferramentas que evitam o vazamento de dados podem falhar. Esse cenário cria

falhas que vão contra os requisitos de acesso e proteção estabelecidos pela LGPD (Cordeiro; Sobral, 2024; De Oliveira *et al.*, 2019).

Em relação às restrições de memória, a escassez de RAM e armazenamento impedem que muitos dispositivos executem a pilha TCP/IP completa ou protocolos de aplicação que já vêm com segurança própria, como MQTT e CoAP (De Oliveira *et al.*, 2019; Rodrigues, 2025). Essa limitação torna os equipamentos suscetíveis a ataques de *software*, como o estouro de *buffer* (*buffer overflow*); dificulta o registro do que acontece no dispositivo (*logs*); e a gestão de chaves de criptografia, que são essenciais para conferir o que foi feito com as informações (Rodrigues, 2025; Sousa; Silva, 2025; Araujo, 2023).

Além disso, o consumo de energia também é uma barreira, visto que grande parte desses dispositivos possui baterias que duram pouco. Usar protocolos de proteção conhecidos, como TLS ou DTLS, pode gastar muita bateria e deixar a rede lenta. Isso pode dificultar o uso de conversas protegidas por código em aparelhos muito limitados (Soares; Alencar, 2025).

Por causa desses problemas, os dados acabam sendo enviados sem proteção ou com senhas fracas. Isso facilita ataques de invasores que interceptam mensagens (*man-in-the-middle*) ou derrubam o serviço (DoS), colocando em risco a privacidade e a segurança das informações dos usuários (De Oliveira *et al.*, 2019; Sousa; Silva, 2025).

Portanto, as limitações de processamento, memória e energia representam desafios significativos para a segurança em IoT, tornando necessária a adoção de mecanismos de proteção compatíveis com as restrições desses dispositivos.

2.5 LGPD E OS DESAFIOS DA PROTEÇÃO DE DADOS NA IOT

A Lei Geral de Proteção de Dados Pessoais (LGPD), publicada em 2018 (Lei nº 13.709/2018), é fundamental para compreender como o Brasil estrutura a proteção de dados em um cenário cada vez mais conectado, especialmente diante do avanço da IoT.

Articulada ao Plano Nacional de Internet das Coisas (Decreto nº 9.854/2019) para fortalecer o uso ético e seguro de informações em ambientes conectados, a LGPD estabelece diretrizes para a coleta e o tratamento de dados, a fim de proteger a privacidade dos usuários (GOV.BR, 2024).

O objeto central da norma é o dado pessoal, definido como qualquer informação relacionada a uma pessoa natural identificada ou identificável (Costa, 2022). Essa definição ampla, como defende Alencar (2023), garante que a LGPD alcance todas as entidades, públicas ou privadas, que processam dados de cidadãos brasileiros.

Ao relacionar a LGPD à IoT, percebe-se que os desafios de implementação são maiores do que os encontrados em tecnologias tradicionais. Isso ocorre porque os dispositivos IoT permanecem constantemente conectados e realizam a coleta contínua de dados, muitos deles sensíveis, gerando um grande volume de informações e tornando mais complexo o controle e o gerenciamento (Calaza, 2024).

Para orientar o tratamento dessas informações, a LGPD estabelece princípios essenciais (Art. 6º). Segundo Agostinelli (2018), esses princípios também servem como base para compreender os desafios enfrentados pelas organizações na aplicação da lei em ambientes IoT, dentre os quais destacam-se:

- **Segurança e Prevenção:** A diversidade das redes e a limitação técnica de muitos dispositivos dificultam a aplicação de medidas de proteção, o que eleva o risco de invasões e incidentes de segurança (Bianchini; Silva; Dias, 2024; Costa, 2022).
- **Finalidade, Adequação e Necessidade:** Enquanto a IoT opera com base na coleta massiva de dados para análises futuras, a LGPD exige que o tratamento se limite ao mínimo necessário para fins específicos. Esse contraste pode gerar conflitos com a lógica de funcionamento de muitos sistemas inteligentes (Bianchini; Silva; Dias, 2024).
- **Transparência e Livre Acesso:** Garantir que o titular compreenda o tratamento de seus dados é um desafio em ambientes onde a coleta é automática (passiva) e o processamento utiliza algoritmos complexos de Inteligência Artificial (IA) e *Machine Learning* (Costa, 2022).

Outro obstáculo da implementação da LGPD no ecossistema da IoT reside na falta de padronização dessas tecnologias, dificultando a criação de um ambiente regulatório uniforme (Costa, 2022).

Soma-se a isso a existência de uma lacuna legislativa, uma vez que a LGPD não apresenta diretrizes específicas para o tratamento de dados em sistemas de IoT,

levando as organizações a realizarem uma aplicação analógica dos princípios da lei, (Bianchini; Silva; Dias, 2024).

Dessa forma, embora a LGPD estabeleça princípios fundamentais para a proteção de dados pessoais, sua aplicação no contexto da IoT enfrenta desafios técnicos, regulatórios e operacionais. Esse cenário evidencia a necessidade de estratégias específicas que permitam conciliar inovação tecnológica, conformidade legal e segurança da informação.

3 PROCEDIMENTOS METODOLÓGICOS

3.1 CARACTERIZAÇÃO DA PESQUISA

Quanto à abordagem, esta pesquisa se enquadra como qualitativa. Segundo Marconi e Lakatos (2024), esse tipo de estudo foca na análise de conteúdos e significados para compreender a complexidade das características. Essa abordagem permite interpretar conceitos, identificar desafios, examinar perspectivas dos autores e compreender como a literatura discute a relação entre IoT e privacidade

Em relação aos objetivos, o estudo possui caráter exploratório e descritivo. Conforme as definições de Gil (2026) e Marconi e Lakatos (2024), as pesquisas exploratórias buscam maior familiaridade com o problema, enquanto as descritivas detalham as características de um fato. Assim, o trabalho explorou o cenário atual de riscos na IoT e descreveu os mecanismos de segurança propostos pela literatura para amenizar essas falhas.

Quanto aos procedimentos técnicos, a pesquisa caracterizou-se como bibliográfica. Gil (2026) destaca que esse procedimento é fundamental para a construção do conhecimento científico, pois utiliza a revisão da literatura para fundamentar o estudo. Este trabalho foi desenvolvido a partir da análise de artigos científicos, dissertações, teses e demais publicações relacionadas à IoT, segurança da informação, privacidade, criptografia e LGPD.

3.2 ESTRATÉGIA DE BUSCA

3.2.1 BASES DE DADOS

A coleta dos dados foi realizada por meio de uma revisão sistematizada da literatura. As buscas foram conduzidas nas bases de dados Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), Google Acadêmico e Sociedade Brasileira de Computação (SBC).

Para isso, foram utilizados descritores combinados por meio dos operadores booleanos AND e OR, visando ampliar e refinar os resultados conforme a relevância para o tema da pesquisa, conforme o Quadro 1.

Quadro 1 – Strings de busca utilizadas nas bases de dados

DESCRIÇÃO	STRING DE BUSCA
Busca 1	("Internet das Coisas" OR "IoT") AND ("segurança da informação") AND ("privacidade na IoT" OR "proteção de dados")
Busca 2	("Internet das Coisas" OR "IoT") AND ("Lei Geral de Proteção de Dados Pessoais" OR "LGPD")
Busca 3	("Internet das Coisas" OR "IoT") AND ("criptografia" OR "mecanismos de segurança")
Busca 4	("Internet das Coisas" OR "IoT") AND ("segurança da informação") AND ("LGPD" OR "proteção de dados")

Fonte: Elaborado pela autora (2026).

Como delimitação temporal, foram considerados estudos publicados entre 2019 e 2026, com o objetivo de contemplar produções científicas recentes. Excepcionalmente usou-se uma fonte de 2018 por ser considerada relevante.

3.2.2 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO

Após a realização das buscas, os materiais passaram por uma triagem inicial baseada na leitura dos títulos, resumos e palavras-chave. Posteriormente, os estudos potencialmente relevantes foram submetidos à leitura na íntegra.

Como critérios de inclusão, foram considerados artigos científicos,

dissertações e teses publicados entre 2019 e 2026, disponíveis na íntegra e que abordassem diretamente temas relacionados à Internet das Coisas, vulnerabilidades dos dispositivos, segurança da informação, privacidade em IoT ou à LGPD.

Foram excluídos trabalhos duplicados, estudos indisponíveis na íntegra, publicações que não apresentavam relação direta com os objetivos da pesquisa e materiais sem caráter científico, como notícias, blogs e conteúdos opinativos.

3.3 PROCESSO DE ANÁLISE DOS DADOS

Após a seleção do material, os dados foram examinados por meio de uma revisão qualitativa, permitindo a identificação de padrões, conceitos recorrentes e principais contribuições teóricas sobre a temática. Esse processo também possibilitou organizar, de forma sistemática, as informações extraídas dos estudos.

A análise foi orientada pelos objetivos da pesquisa, buscando compreender como a literatura descreve os riscos presentes na IoT, de que forma esses riscos impactam a privacidade dos usuários e quais diretrizes a legislação brasileira oferece para mitigar tais vulnerabilidades.

4 RESULTADOS E DISCUSSÃO

Com base na análise dos estudos selecionados, foram identificadas as principais restrições relacionadas aos dispositivos IoT, bem como as soluções propostas na literatura para mitigar essas limitações. O Quadro 2 apresenta uma síntese dos resultados obtidos, relacionando as restrições de processamento, memória e consumo de energia às respectivas estratégias de segurança apontadas pelos autores analisados.

Quadro 2 – Relação entre restrições técnicas da IoT e soluções propostas

RESTRIÇÃO	POSSÍVEL SOLUÇÃO	REFERÊNCIA
Processamento limitado	Utilização de protocolos leves de comunicação (MQTT) e criptografia leve para reduzir o custo computacional dos mecanismos de segurança.	Araujo (2023); Cordeiro e Sobral (2024); Rodrigues

		(2025); Soares e Alencar (2025).
Memória limitada	Emprego de criptografia leve e utilização de gateways para centralizar funções de segurança, reduzindo a demanda por memória dos dispositivos IoT.	Araujo (2023); Cordeiro e Sobral (2024).
Alto consumo de energia	Adoção de criptografia leve, projetada para dispositivos restritos, reduzindo o consumo de energia sem comprometer a segurança.	Araujo (2023); Soares e Alencar (2025).

Fonte: Elaborado pela autora (2026).

Em relação às limitações de processamento, observou-se consenso entre os estudos analisados quanto à necessidade de empregar soluções compatíveis com a reduzida capacidade computacional desses equipamentos. Rodrigues (2025) destaca a utilização de protocolos leves de comunicação, como MQTT, para reduzir o processamento necessário à troca de mensagens, aliados à adoção de medidas de segurança integradas à infraestrutura da rede.

De forma complementar, Araujo (2023), Cordeiro e Sobral (2024) e Soares e Alencar (2025) apontam a criptografia leve como uma alternativa adequada, uma vez que reduz o custo computacional dos mecanismos de segurança e possibilita sua implementação em dispositivos com recursos limitados.

Sob a perspectiva da LGPD, a adoção dessas soluções contribui para o atendimento do princípio da segurança, previsto no Art. 6º da lei, ao favorecer a implementação de mecanismos capazes de proteger os dados pessoais contra acessos não autorizados, mesmo em dispositivos com restrições de processamento.

Quanto às limitações de memória, os estudos indicam que os mecanismos de segurança devem considerar a reduzida capacidade de memória dos dispositivos IoT. Araujo (2023) destaca a criptografia leve como uma alternativa adequada, por ter sido desenvolvida para ambientes com recursos restritos, reduzindo a demanda por memória e outros recursos computacionais.

Além disso, Cordeiro e Sobral (2024) propõem a utilização de gateways de segurança para centralizar o processamento das informações, reduzindo a sobrecarga dos dispositivos mais restritos e favorecendo uma comunicação segura em redes heterogêneas.

Nesse contexto, os gateways e a criptografia leve também auxiliam as organizações na conformidade com a LGPD, ao fortalecerem a proteção dos dados pessoais durante o armazenamento e a transmissão das informações, reduzindo riscos de incidentes de segurança e favorecendo o cumprimento das medidas técnicas exigidas pela legislação.

No que se refere ao consumo de energia, os estudos analisados apontam a criptografia leve como a principal alternativa para atender às restrições energéticas dos dispositivos IoT. Soares e Alencar (2025) afirmam que esse tipo de criptografia reduz o consumo energético em comparação às criptografias tradicionais, preservando a segurança da comunicação entre os dispositivos. De maneira semelhante, Araujo (2023) ressalta que a criptografia leve é projetada para dispositivos com recursos limitados.

Assim, observa-se que a redução do consumo energético não ocorre em detrimento da segurança, permitindo que os dispositivos mantenham mecanismos de proteção ativos por mais tempo e contribuindo para que o tratamento dos dados pessoais esteja alinhado às exigências de segurança estabelecidas pela LGPD.

5 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo analisar de que forma as limitações técnicas dos dispositivos IoT influenciam a adequação às diretrizes da LGPD, considerando seus impactos na proteção da privacidade dos usuários em ambientes conectados.

Nesse sentido, a partir da revisão sistematizada da literatura, verificou-se que restrições relacionadas ao processamento, memória e consumo de energia representam desafios para a implementação de mecanismos de segurança compatíveis com os requisitos da legislação.

Os estudos analisados evidenciaram que soluções como protocolos leves de comunicação, criptografia leve e gateways de segurança contribuem para minimizar essas limitações, fortalecendo a proteção das informações e favorecendo o

atendimento às exigências da LGPD, especialmente no que se refere à implementação de medidas de segurança para o tratamento de dados pessoais.

Dessa forma, conclui-se que a conformidade com a LGPD depende não apenas do atendimento aos requisitos legais, mas também da adoção de soluções técnicas compatíveis com as limitações dos dispositivos IoT, capazes de fortalecer a segurança da informação e reduzir riscos à privacidade dos usuários.

Por fim, considera-se que os objetivos propostos foram alcançados, permitindo compreender a relação entre as limitações técnicas da IoT, a segurança da informação e a proteção da privacidade. Como limitação, destaca-se que a pesquisa foi desenvolvida exclusivamente por meio de revisão da literatura. Assim, sugere-se que estudos futuros realizem avaliações práticas das soluções identificadas, analisando sua aplicação em diferentes cenários de Internet das Coisas.

REFERÊNCIAS

AGOSTINELLI, Joice. **A importância da lei geral de proteção de dados pessoais no ambiente online.** *ETIC – Encontro de Iniciação Científica*, v. 21, 2018. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7025>. Acesso em: 5 nov. 2025.

ALENCAR, Larissa Camargo Pinho de. **Lei geral de proteção de dados – LGPD e segurança na internet.** *Revista Judicial Brasileira*, v. 3, 2023. Disponível em: <https://revistadaenfam.emnuvens.com.br/renfam/article/view/232>. Acesso em: 27 abr. 2026.

ALVES, David; PEIXOTO, Mario; ROSA, Thiago. **Internet das Coisas (IoT): segurança e privacidade dos dados pessoais.** Rio de Janeiro: Alta Books, 2021.

ARAÚJO, Alex Rodrigues. **Métodos e técnicas de segurança para dispositivos IoT: uma revisão sistemática da literatura.** 2023. Trabalho de Conclusão de Curso (Tecnologia em Telemática) – Instituto Federal da Paraíba, Campus Campina Grande, Campina Grande, 2023. Disponível em: <https://repositorio.ifpb.edu.br/handle/177683/3547>. Acesso em: 27 abr. 2026.

BIANCHINI, Brian Melinski; SILVA, Erik Faria; DIAS, Jônatas Cerqueira. **Proteção de privacidade em dispositivos IoT de acordo com a LGPD: Um estudo abrangente.** *Revista Processando o Saber*, Praia Grande, v. 16, 2024. Disponível em: <https://fatecpg.edu.br/revista/index.php/ps/article/view/346>. Acesso em: 27 abr. 2026.

BRASIL. **Os quatro pilares da segurança da informação – confidencialidade, disponibilidade, integridade e autenticidade.** Brasília, DF: Laboratório Nacional de Computação Científica (LNCC), 2024. Disponível em: <https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao/os-quatro-pilares-da-seguranca-da-informacao-2013-confidencialidade-disponibilidade-integridade-e-autenticidade>. Acesso em: 5 nov. 2025.

BRASIL. **Plano Nacional de Internet das Coisas. Governo Digital – Estratégias e Políticas Digitais.** Brasília: Governo Federal, 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/plano-nacional-de-internet-das-coisas>. Acesso em: 5 nov. 2025.

CALAZA, Tales. **Evolução e regulação da privacidade e proteção de dados no contexto da internet das coisas no cenário brasileiro.** *Revista do CAAP*, v. 29, 2024. Disponível em: <https://periodicos.ufmg.br/index.php/caap/article/view/52353>. Acesso em: 7 nov. 2025.

CARVALHO, Cristiana. **Internet das coisas: entenda o que é e como funciona.** Tecmundo, 2020. Disponível em: <https://www.tecmundo.com.br/internet/230884-internet-coisas-entenda-funciona.htm>. Acesso em: 6 nov. 2025.

CORDEIRO, Antonio Alisio de Meneses; SOBRAL, Leandro Lima. **Desafios Regulatórios da Lei Geral de Proteção de Dados (LGPD) para Internet das Coisas (IoT)**. Revista Tecnologia, Fortaleza, v. 45, 2024. Disponível em: <https://ojs.unifor.br/tec/article/view/13998>. Acesso em 29 abr. 2026.

COSTA, Renato Brito. **A Lei Geral de Proteção de Dados Pessoais aplicada à Internet das Coisas: uma revisão sistemática**. 2022. Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) – Universidade Federal do Ceará, Campus Sobral, Sobral, 2022. Disponível em: <https://repositorio.ufc.br/handle/riufc/66631>. Acesso em 29 abr. 2026.

DACHYAR, Muhammad; ZAGLOEL, Teuku Yuri M.; SARAGIH, L. Ranjaliba. **Crescimento e desenvolvimento do conhecimento: pesquisa da Internet das Coisas (IoT), 2006–2018**. *Heliyon*, v. 5, 2019. Disponível em: [https://www.cell.com/heliyon/fulltext/S2405-8440\(19\)35924-9](https://www.cell.com/heliyon/fulltext/S2405-8440(19)35924-9). Acesso em 29 abr. 2026.

DE OLIVEIRA, Nairobi Spiecker *et al.* **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*, v. 17, 2019. Disponível em: <https://journals-sol.sbc.org.br/index.php/reic/article/view/1704>. Acesso em 30 abr. 2026.

FORNASIER, Mateus de Oliveira. **A aplicabilidade da Internet das Coisas (IoT) entre os direitos fundamentais à saúde e à privacidade**. *Revista de Investigações Constitucionais*, 2020. Disponível em: <https://revistas.ufpr.br/rinc/article/view/67592>. Acesso em: 6 nov. 2025.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 8. ed. São Paulo: Atlas, 2026.

IBM. **O que é segurança da informação (InfoSec)?** IBM – Think, 2024. Disponível em: <https://www.ibm.com/br-pt/think/topics/information-security>. Acesso em: 5 nov. 2025.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia científica**. 8. ed. Barueri, SP: Atlas, 2024. xvi, ISBN 9786559770656.

PANEK, Lin Cristina Tung. **Lei geral de proteção de dados nº 13.709/2018: uma análise dos principais aspectos e do conceito de privacidade na sociedade informacional**. 2019. Disponível em: <https://acervodigital.ufpr.br/handle/1884/68114>. Acesso em: 5 nov. 2025.

ROCHA NETO, Carlos Mariano de Souza *et al.* **Segurança na Internet das Coisas: um estudo avaliativo sobre vulnerabilidades e estratégias de mitigação**. Caminhos da Pesquisa Multidisciplinar, cap. 4, 2025. Disponível em: <https://aurumpublicacoes.com/index.php/editora/article/view/639>. Acesso em 30 abr. 2026.

RODRIGUES, Thaís Adrielle Ferreira. **Vulnerabilidades em Protocolos de Aplicação para Dispositivos IoT**. 2025. Trabalho de Conclusão de Curso (Graduação em Segurança da Informação) – Universidade Federal do Ceará, Itapajé, 2025. Disponível em: <https://repositorio.ufc.br/handle/riufc/80350>. Acesso em 30 abr. 2026.

SIQUEIRA, Oniye Nashara *et al.* **A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD**. *Revista Eletrônica Pesquiseduca*, v. 13, 2021. Disponível em: <http://periodicos.unisantos.br/pesquiseduca/article/view/1029>. Acesso em: 10 nov. 2025.

SOARES, Ítalo Rodrigo Monte; ALENCAR, Saylon Ferreira. **Protocolos de segurança para Internet das Coisas (IoT)**. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 12, 2025. Disponível em: <https://periodicorease.pro.br/rease/article/view/22900>. Acesso em 25 abr. 2026.

SOUSA, Iranildo Chagas de; SILVA, Danilo Borges da. **A segurança dos dispositivos IOT e outras vulnerabilidades podem ser exploradas por hackers**. 2025. Trabalho de Conclusão de Curso (Ciência da Computação) – Universidade Estadual do Piauí, Floriano, 2025. Disponível em: <https://sistemas2.uespi.br/handle/tede/1050>. Acesso em 25 abr. 2026.