



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
DEPARTAMENTO DE ENGENHARIAS E TECNOLOGIA
CURSO INTERDISCIPLINAR EM TECNOLOGIA DA INFORMAÇÃO

FRANCISCO DIOGO DA COSTA SILVA

**ABORDAGENS DE PRIVACIDADE EM DISPOSITIVOS IoT SOB A ÓTICA DA
CONFORMIDADE COM A LGPD: UM MAPEAMENTO SISTEMÁTICO**

PAU DOS FERROS

2025

FRANCISCO DIOGO DA COSTA SILVA

**ABORDAGENS DE PRIVACIDADE EM DISPOSITIVOS IoT SOB A ÓTICA DA
CONFORMIDADE COM A LGPD: UM MAPEAMENTO SISTEMÁTICO**

Monografia apresentada à Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Tecnologia da Informação.

Orientador: João Batista de Souza Neto, Prof. Dr.

PAU DOS FERROS

2025

© Todos os direitos estão reservados a Universidade Federal Rural do Semi-Árido. O conteúdo desta obra é de inteira responsabilidade do (a) autor (a), sendo o mesmo, passível de sanções administrativas ou penais, caso sejam infringidas as leis que regulamentam a Propriedade Intelectual, respectivamente, Patentes: Lei nº 9.279/1996 e Direitos Autorais: Lei nº 9.610/1998. O conteúdo desta obra tomar-se-á de domínio público após a data de defesa e homologação da sua respectiva ata. A mesma poderá servir de base literária para novas pesquisas, desde que a obra e seu (a) respectivo (a) autor (a) sejam devidamente citados e mencionados os seus créditos bibliográficos.

S586a Silva, Francisco Diogo da Costa.
Abordagens de privacidade em dispositivos IoT
sob a ótica da conformidade com a LGPD: um
mapeamento sistemático / Francisco Diogo da
Costa Silva. - 2025.
62 f. : il.

Orientador: João Batista de Souza Neto Neto.
Monografia (graduação) - Universidade Federal
Rural do Semi-árido, Curso de Tecnologia da
Informação, 2025.

1. Internet das Coisas. 2. LGPD. 3.
Privacidade. 4. Mapeamento Sistemático . I. Neto,
João Batista de Souza Neto , orient. II. Título.

Ficha catalográfica elaborada por sistema gerador automático em conformidade
com AACR2 e os dados fornecidos pelo(a) autor(a).

Biblioteca Campus Pau dos Ferros
Bibliotecária: Erlanda Maria Lopes da Silva
CRB: 15/966

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC's) foi desenvolvido pelo Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) e gentilmente cedido para o Sistema de Bibliotecas da Universidade Federal Rural do Semi-Árido (SISBI-UFERSA), sendo customizado pela Superintendência de Tecnologia da Informação e Comunicação (SUTIC) sob orientação dos bibliotecários da instituição para ser adaptado às necessidades dos alunos dos Cursos de Graduação e Programas de Pós-Graduação da Universidade.

FRANCISCO DIOGO DA COSTA SILVA

**ABORDAGENS DE PRIVACIDADE EM DISPOSITIVOS IoT SOB A ÓTICA DA
CONFORMIDADE COM A LGPD: UM MAPEAMENTO SISTEMÁTICO**

Monografia apresentada à Universidade
Federal Rural do Semi-Árido como requisito
para obtenção do título de Bacharel em
Tecnologia da Informação.

Defendida em: 01 / 08 / 2025

BANCA EXAMINADORA

João Batista de Souza Neto, Prof. Dr. (UFERSA)
Presidente

George Felipe Fernandes Vieira, Prof. (UFERSA)
Membro Examinador

Bruno Borges da Silva, Prof. Esp. (UFERSA)
Membro Examinador

DEDICATÓRIA

Dedico este trabalho a todos que acreditaram em mim durante essa caminhada, em especial à minha amada esposa, que foi minha guia, minha inspiração e minha força ao longo da graduação. Com sua inteligência e companheirismo, ela trouxe sentido a minha vida, sendo mais que fundamental para a realização desta conquista.

AGRADECIMENTOS

Primeiramente, agradeço a Jeová Deus, por me conceder vida, forças e sabedoria ao longo de toda essa jornada acadêmica. Sem Sua presença e direção, nada disso teria sido possível.

Aos meus pais e à minha família, por todo o incentivo ao longo dos anos. Foram eles que me ensinaram o valor da perseverança, da humildade e do esforço.

À minha esposa, Lorena, por sua paciência, compreensão e suporte em todos os momentos, especialmente nos mais difíceis e cansativos, foi nesses momentos que encontrei forças em ti e no seu amor. Sua presença foi essencial para que eu seguisse em frente com determinação e coragem, sempre me lembrando todos os dias do porquê vale a pena persistir.

Agradeço ao meu orientador, João Batista, por ter me dedicado sua orientação com atenção e paciência. Sua orientação e conhecimento foram essenciais para a concretização deste trabalho.

Por fim, agradeço a todos os colegas e professores que contribuíram para minha formação, muito obrigado.

RESUMO

A crescente presença de dispositivos conectados à Internet das Coisas (IoT) impõe novos desafios à proteção da privacidade e à conformidade com legislações como a Lei Geral de Proteção de Dados Pessoais (LGPD). Este trabalho tem como objetivo identificar e analisar as abordagens de privacidade adotadas em dispositivos IoT sob a ótica da conformidade com a LGPD, por meio de um mapeamento sistemático da literatura científica. A pesquisa inclui definição de critérios de inclusão e exclusão, elaboração de string de busca, seleção em bases e extração de dados. Ao todo, foram analisados 23 estudos que discutem a aplicação de mecanismos técnicos, organizacionais e legais para garantir a proteção de dados em ambientes IoT. Os resultados mostram algumas estratégias, com destaque para o uso de anonimização, controle de consentimento, blockchain, criptografia e modelos baseados em governança de dados. A análise revelou ainda lacunas na aplicação prática da LGPD, especialmente em contextos com volume de dados sensíveis. Conclui-se que a conformidade entre IoT e LGPD demanda esforços integrados entre áreas técnicas e jurídicas, sendo necessária a contínua atualização de soluções frente às mudanças tecnológicas e regulatórias.

Palavras-chave: internet das coisas; LGPD; privacidade; mapeamento sistemático.

ABSTRACT

The growing presence of devices connected to the Internet of Things (IoT) poses new challenges to privacy protection and compliance with legislation such as the General Data Protection Law (LGPD). This study aims to identify and analyze the privacy approaches adopted in IoT devices from the perspective of LGPD compliance, through a systematic mapping of the scientific literature. The research includes defining inclusion and exclusion criteria, developing search strings, selecting databases, and extracting data. In total, 23 studies were analyzed that discuss the application of technical, organizational, and legal mechanisms to ensure data protection in IoT environments. The results reveal several strategies, highlighting the use of anonymization, consent control, blockchain, encryption, and data governance-based models. The analysis also revealed gaps in the practical application of the LGPD, especially in contexts with a large volume of sensitive data. It is concluded that compliance between IoT and LGPD requires integrated efforts between technical and legal departments, requiring the continuous updating of solutions in the face of technological and regulatory changes.

Keywords: internet of things; LGPD; privacy; systematic mapping.

LISTA DE FIGURAS

Figura 1 - O Processo de Mapeamento Sistemático.....	26
--	----

LISTA DE GRÁFICOS

Gráfico 1 – Abordagens Propostas nos Estudos.....	40
Gráfico 2 – Aplicações encontradas nos estudos analisados.....	41
Gráfico 3 – Desafios encontrados nos estudos analisados.....	43
Gráfico 4 – Abordagens exploradas ao longo dos anos.....	44
Gráfico 5 – Aplicações exploradas ao longo dos anos.....	44
Gráfico 6 – Desafios exploradas ao longo dos anos.....	45
Gráfico 7 - Tipos de trabalhos científicos.....	50
Gráfico 8 - Anos de publicação dos estudos.....	51
Gráfico 9 - Locais de afiliação dos autores nacionais.....	52
Gráfico 10 - Locais de afiliação dos autores internacionais.....	52

LISTA DE TABELAS

Tabela 1 – Comparação dos Trabalhos Relacionados.....	25
Tabela 2 – Documentos retornados por base de busca.....	30
Tabela 3 – Resultado dos documentos retornados na Fase 2.....	32
Tabela 4 – Resultado dos documentos retornados na Fase Final.....	33
Tabela 5 - Análise dos estudos aprovados.....	34
Tabela 6 - Faceta: Abordagens.....	38
Tabela 7 - Faceta: Aplicações referentes aos estudos analisados.....	39
Tabela 8 - Faceta: Desafios enfrentados nos estudos.....	40

LISTA DE ABREVIATURAS E SIGLAS

IoT	Internet das Coisas
LGPD	Lei Geral de Proteção de Dados
MSL	Mapeamento Sistemático da Literatura
RS	Revisão Sistemática
GDPR	Regulamento Geral de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
ID	Identificador
ABNT	Associação Brasileira de Normas Técnicas
SUS	Sistema Único de Saúde
PDS	Personal Data Store
PbD	Privacy by Design
PII	Informações de identificação pessoal
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
ACM	Association for Computing Machinery

SUMÁRIO

1 INTRODUÇÃO.....	14
1.1 Problematização.....	14
1.2 Justificativa.....	15
1.3 Objetivos.....	16
1.3.1 Objetivo Geral.....	16
1.3.2 Objetivo Específico.....	16
1.4 Contribuição do trabalho.....	16
1.5 Organização do trabalho.....	17
2 FUNDAMENTAÇÃO TEÓRICA.....	18
2.1 Mapeamento sistemático da literatura.....	18
2.2 Internet das coisas (IoT).....	19
2.3 Lei Geral de Proteção de Dados (LGPD).....	20
3 TRABALHOS RELACIONADOS.....	22
3.1 Internet das coisas e privacidade: uma revisão sistemática de literatura.....	22
3.2 Observabilidade em sistemas de Internet das Coisas: um mapeamento sistemático.	22
3.3 A Lei Geral de Proteção de Dados pessoais aplicada à Internet das Coisas: uma revisão sistemática.....	23
3.4 Dos desafios da implementação da lei geral de proteção de dados no campo de IOT	23
3.5 Internet das Coisas e Big Data na nova Lei de Proteção de Dados: Análise da proteção dos dados sensíveis.....	24
3.6 Considerações finais sobre os trabalhos relacionados.....	24
4 METODOLOGIA.....	26
4.1 Planejamento do mapeamento sistemático.....	26
4.2 Condução do mapeamento sistemático.....	26
4.3 Síntese do processo metodológico.....	27
5 RESULTADOS.....	29
5.1 Questões da pesquisa.....	29
5.2 String de buscas.....	29
5.3 Bases de artigos para pesquisa.....	30
5.4 Critérios de inclusão e exclusão.....	31
5.3.1 Critérios de inclusão.....	31
5.3.2 Critérios de exclusão.....	31
5.5 Desenvolvimento do mapeamento sistemático.....	32
5.6 Esquema de classificação e extração dos dados.....	33
5.7 Análise das respostas.....	40

5.8 Respostas às questões de pesquisa.....	45
5.9 Considerações finais dos resultados.....	53
6 CONSIDERAÇÕES FINAIS.....	55
6.1 Trabalhos futuros.....	55
REFERÊNCIAS.....	57

1 INTRODUÇÃO

A Internet das Coisas (IoT) representa uma inovação tecnológica que marca a conexão de dispositivos físicos como a internet, permitindo a coleta e o compartilhamento de dados em ambientes como residências, cidades, indústrias e hospitais (Atzori; Iera; Morabito, 2010). Nikola Tesla, por exemplo, já visava em 1926 um mundo conectado por dispositivos sem fio, antecipando o que viria a ser uma das bases da IoT atual (Tesla, 1926 apud Carrion; Quaresma, 2019).

A consolidação da IoT se deu a partir da década de 1990, com iniciativas como a criação do primeiro dispositivo conectado à internet e com a popularização do termo “Internet das Coisas” por Kevin Ashton, em 1999 (Carrion; Quaresma, 2019). Desde então, a IoT evoluiu para dispositivos interconectados que vão de sensores industriais a produtos voltados ao consumidor final, como smartwatches, câmeras inteligentes e eletrodomésticos conectados.

A realidade dos produtos está a cada dia mais conectados e transformou a forma como usuários e organizações interagem com a tecnologia, mostrando um cenário em que “coisas” comunicam-se entre si e com os seres humanos. No entanto, essa conectividade também introduz preocupações significativas com relação à segurança e à privacidade dos dados que são gerados. Muitos dispositivos IoT operam de forma invisível aos usuários, utilizando dados como localização, hábitos de consumo e condições de saúde (Carrion; Quaresma, 2019). Nesse contexto, realizar a adoção de medidas de segurança da informação e conformidade legal torna-se fundamental.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, estabelece diretrizes para o tratamento de dados pessoais e impõe obrigações às organizações quanto à transparência, segurança, consentimento e responsabilidade no uso dessas informações. Considerando o impacto da IoT na coleta de dados pessoais, torna-se necessário avaliar como os sistemas baseados em IoT têm sido desenvolvidos ou adaptados para atender aos requisitos da LGPD.

1.1 Problemática

A conformidade com a LGPD representa um desafio importante para projetos que envolvem dispositivos IoT, por apresentar uma complexidade técnica e a diversidade de contextos em que estes dispositivos trabalham. Embora existam iniciativas e soluções voltadas à proteção da privacidade em ambientes IoT, é possível que tenha pouca clareza

sobre quais abordagens estão sendo propostas, implementadas e analisadas na literatura científica.

Embora a Lei Geral de Proteção de Dados (LGPD) estabeleça diretrizes importantes para a proteção da privacidade dos usuários, a sua aplicação prática em dispositivos IoT pode ser um desafio técnico significativo. Segundo Oliveira et al. (2019), a exigência de mecanismos como consentimento informado, controle de acesso, transmissão segura e exclusão de dados entra em conflito com as limitações físicas desses dispositivos, como uma baixa capacidade de processamento, memória e energia. Além disso, muitas dessas soluções trabalham de forma autônoma, o que dificulta o atendimento a obrigações legais como a transparência e o direito de acesso aos dados.

Diante disso, torna-se fundamental compreender quais são as abordagens já existentes e quais dificuldades persistem na literatura científica sobre o tema.

1.2 Justificativa

A crescente integração de dispositivos conectados em setores como saúde, indústria, transporte e residências inteligentes expõe a sociedade a novos riscos relacionados à privacidade e à segurança da informação. Embora a Lei Geral de Proteção de Dados Pessoais (LGPD) tenha estabelecido padrões legais claros para o tratamento de dados pessoais no Brasil, a sua aplicação em ambientes compostos por dispositivos IoT de baixa capacidade computacional permanece um desafio pouco explorado. A IoT, por mais que promova inovação e eficiência, também apresenta riscos à privacidade, especialmente quando envolve dados sensíveis e pessoais (Carrion; Quaresma, 2019).

A literatura científica sobre proteção de dados pessoais apresenta um predomínio de estudos conceituais ou de análise normativa, mas há uma carência de pesquisas que proponham e validem soluções técnicas efetivas para a conformidade com a LGPD em cenários restritos por limitações físicas e computacionais, como ocorre com sensores, atuadores e dispositivos embarcados de pequeno porte. Segundo Oliveira et al. (2019), mecanismos exigidos pela LGPD, como consentimento informado, controle de acesso e exclusão de dados, nem sempre são viáveis em dispositivos IoT devido a limitações técnicas.

Essa lacuna é particularmente relevante porque, sem adaptações técnicas adequadas, a conformidade legal se torna impraticável, o que pode aumentar o risco de violações de privacidade e descumprimento regulatório. Assim, este estudo justifica-se pela necessidade de reunir e analisar, por meio de um mapeamento sistemático, as abordagens de privacidade aplicadas a dispositivos IoT sob a ótica da LGPD, identificando soluções recorrentes,

inovações tecnológicas e barreiras técnicas enfrentadas. Com isso, podendo contribuir para o avanço de pesquisas aplicadas e para o desenvolvimento de soluções práticas.

1.3 Objetivos

Neste trabalho, o foco encontra-se nas abordagens de privacidade de dispositivos IoT sob a perspectiva da conformidade LGPD.

1.3.1 Objetivo Geral

O presente trabalho busca entender como a literatura científica tem abordado a conformidade com a LGPD no contexto da IoT. Levando em consideração os desafios técnicos e legais impostos pela coleta de dados nesses dispositivos, esta pesquisa propõe um mapeamento sistemático com o propósito de identificar, classificar e analisar as abordagens, as áreas de aplicações e os desafios existentes voltadas à proteção da privacidade.

1.3.2 Objetivo Específico

Procurando atender ao que foi descrito no objetivo geral da pesquisa, os seguintes objetivos específicos foram destacados:

- Escolher e definir uma string de busca adequada e aplicá-la nas principais bases científicas da área;
- Analisar e definir os estudos importantes com base em critérios de inclusão e exclusão;
- Coletar e analisar as abordagens de privacidade identificadas nos estudos primários;
- Realizar a análise para a organização dos dados;
- Apontar lacunas de pesquisa e possíveis caminhos para estudos futuros.

1.4 Contribuição do trabalho

Este mapeamento sistemático contribui para o avanço do conhecimento sobre a relação entre privacidade, Internet das Coisas e conformidade legal no Brasil, com o intuito de oferecer uma visão estruturada das abordagens existentes na literatura científica voltadas à adequação dos dispositivos IoT às exigências da LGPD. O mapeamento sistemático realizado possibilita identificar padrões, lacunas e desafios que ainda persistem na implementação prática dessas abordagens.

Além disso, os resultados obtidos podem contribuir com pesquisadores e profissionais da área de tecnologia para a construção de soluções mais eficazes às normas de proteção de dados. Ao reunir, classificar e analisar os estudos primários mais relevantes sobre o tema.

1.5 Organização do trabalho

O presente trabalho está organizado em seis capítulos, estruturados para facilitar a compreensão dos objetivos, metodologia e resultados obtidos. O Capítulo 2 traz a fundamentação teórica, com a definição dos principais conceitos relacionados à Internet das Coisas (IoT), também sobre a Lei Geral de Proteção de Dados (LGPD) e também são apresentados os princípios do mapeamento sistemático da literatura. No Capítulo 3, são apresentados trabalhos relacionados que abordam sobre privacidade em dispositivos IoT e conformidade com a LGPD. O Capítulo 4 detalha a metodologia utilizada no estudo, descrevendo o planejamento do mapeamento sistemático, os critérios de inclusão e exclusão, as strings de busca utilizadas, a extração de dados e a síntese metodológica. O Capítulo 5 concentra-se na apresentação e análise dos resultados, incluindo a seleção de artigos, onde são discutidas as abordagens de privacidade identificadas, os contextos de aplicação, as lacunas existentes e as respostas às questões de pesquisa propostas. Por fim, o Capítulo 6 apresenta as considerações finais do trabalho, destacando as principais contribuições da pesquisa e propondo recomendações para estudos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

O objetivo deste capítulo é apresentar os conceitos fundamentais para o entendimento deste trabalho. Serão apresentados os principais conceitos sobre Internet das Coisas (IoT), Lei Geral de Proteção de Dados Pessoais (LGPD) e Mapeamento Sistemático da Literatura (MSL).

2.1 Mapeamento sistemático da literatura

O mapeamento sistemático da literatura (MSL) é um estudo no qual o seu objetivo é fornecer uma ampla visão de um campo de pesquisa, organizando e classificando os estudos primários já existentes sobre determinados tópicos (Kitchenham; Charters, 2007). Ao contrário da Revisão Sistemática (RS), que foca na síntese de resultados com profundidade, o MSL busca mapear a amplitude e a essência da produção científica em um tema mais amplo, facilitando a detecção de tendências, falhas e áreas promissoras para investigações futuras (Petersen et al., 2015; Wholin et al., 2013).

Segundo Falbo (2018), o mapeamento sistemático segue um processo estruturado e replicável, dividido em três etapas principais: planejamento, que envolve a definição do protocolo e das questões de pesquisa; condução, que inclui a busca nas bases, a utilização de critérios de seleção e a extração dos dados; e apresentação, na qual os resultados são organizados em categorias e apresentados em forma de tabelas, gráficos ou mapas conceituais.

Uma das formas de colaboração do MSL é ajudar na compreensão do estado da arte de algum domínio, sendo especialmente útil para os pesquisadores que estão na etapa inicial de estudos (Falbo, 2018). Ele também serve de base para a estruturação de revisões sistemáticas mais específicas ou para a proposição de novas pesquisas que preencham lacunas identificadas.

A realização de um MSL requer rigor metodológico, incluindo a elaboração de uma string de busca adequada, a seleção cuidadosa dos estudos com base em critérios de inclusão e exclusão, e a categorização consistente dos resultados. É comum que sejam utilizadas ferramentas de apoio, como planilhas ou softwares especializados, para que se possa certificar a qualidade do processo.

2.2 Internet das coisas (IoT)

A Internet das Coisas (IoT, do inglês *Internet of Things*) é uma das referências tecnológicas que aborda objetos físicos conectados à internet, permitindo a coleta, o processamento e o compartilhamento automático de dados, sem necessidade de intervenção humana constante. Essa tecnologia permite transformar objetos comuns em dispositivos inteligentes, capazes de interagir com o ambiente e com outros sistemas por meio de sensores, atuadores e conectividade em rede (Atzori; Iera; Morabito, 2010).

Por mais que o termo “IoT” tenha sido citado por Kevin Ashton em 1999, Carrion e Quaresma (2019) destacam que em 1926, Nikola Tesla já previa um mundo no qual o ser humano poderia se comunicar com qualquer pessoa, em qualquer lugar, por meio de dispositivos portáteis e sem fio. Ao longo das décadas, essa visão tornou-se realidade, principalmente com os avanços em computação embarcada e redes móveis.

Nos dias atuais, a IoT encontra aplicações em diversos domínios, como cidades inteligentes, agricultura de precisão, logística, automação industrial, saúde digital, monitoramento ambiental e residências inteligentes. Dispositivos como lâmpadas conectadas, câmeras IP, pulseiras fitness, fechaduras eletrônicas e sensores industriais são exemplos comuns desse ecossistema.

Vantagens e benefícios da IoT

A Internet das Coisas oferece benefícios importantes tanto para consumidores quanto para empresas. Entre as vantagens mais relevantes, destaca-se a capacidade de coleta de grandes volumes de dados (*big data*), os quais buscam compreender melhor o comportamento dos usuários, otimizar processos e apoiar decisões estratégicas. A automação também contribui para a economia de recursos, como energia elétrica, por meio de dispositivos que se ativam ou desativam automaticamente com base na presença humana (De Godoi; Araújo, 2019). A IoT também promove ganhos em eficiência operacional, controle remoto de ambientes, melhoria na experiência do usuário e na prestação de serviços públicos e privados, além de abrir novas oportunidades de negócios.

Desvantagens e preocupações com segurança e privacidade

No entanto, a IoT também levanta algumas preocupações relacionadas à segurança da informação e à privacidade dos usuários. A presença constante desses dispositivos, estabelece a sua limitada capacidade de processamento e armazenamento, tornando vulneráveis a

ataques, vazamentos e falhas de proteção de dados. Além disso, muitos dispositivos coletam dados sensíveis sem total transparência ao usuário, o que aumenta o debate sobre o uso dessas tecnologias (Carrion; Quaresma, 2019).

De acordo com De Godoi e Araújo (2019), a privacidade do usuário é um dos pontos críticos da IoT. A coleta de dados muitas vezes ocorre sem um benefício claro para o consumidor, como no caso de eletrodomésticos conectados e, ainda assim, permite ao fabricante mapear o estilo de vida e os hábitos pessoais dos usuários. A posse e o uso indevido desses dados podem trazer riscos significativos à privacidade e à integridade dos indivíduos.

Além disso, a segurança digital é uma preocupação constante. Como mencionam Moraes et al. (2022), os dispositivos IoT estão expostos a diversos tipos de ataques, tanto físicos quanto lógicos. Ataques de software, como exploração de falhas e vulnerabilidades, podem conceder acesso não autorizado a redes inteiras. Já os ataques físicos envolvem a alteração de dispositivos para acessar informações sensíveis.

Diante desses riscos, algumas técnicas de proteção vêm sendo empregadas, sendo a criptografia uma das mais importantes. Segundo Stallings (2015), a criptografia moderna utiliza cifras de bloco para codificar blocos inteiros de dados, dificultando sua leitura por agentes não autorizados. Essas ferramentas são fundamentais durante todas as fases do ciclo de vida da informação: coleta, transmissão e armazenamento.

No entanto, implementar criptografia e outros métodos de proteção em dispositivos com recursos computacionais limitados continua sendo um dos maiores desafios técnicos da área. Como destaca Fukuda (2019), é preciso garantir tanto a segurança física dos dispositivos quanto a proteção lógica das informações sensíveis, respeitando os princípios da confidencialidade, integridade e disponibilidade

2.3 Lei Geral de Proteção de Dados (LGPD)

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece diretrizes sobre o tratamento de dados pessoais no Brasil. Inspirada em legislações internacionais como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD busca garantir o direito à privacidade, à proteção e à autodeterminação informativa dos cidadãos brasileiros (Brasil, 2018).

A lei define dado pessoal como qualquer informação relacionada a pessoa natural identificada ou identificável, incluindo os chamados dados sensíveis, informações sobre

origem racial, convicção religiosa, dados genéticos ou biométricos, entre outros. O tratamento desses dados compreende operações como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018).

A LGPD atribui aos titulares dos dados uma série de direitos, como o acesso, a correção, a portabilidade, a exclusão, a revogação do consentimento e a explicação sobre decisões automatizadas. Por outro lado, os agentes de tratamento, controladores e operadores, são obrigados a adotar medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados, vazamentos e tratamentos ilícitos.

A gestão da conformidade e a fiscalização do cumprimento da LGPD são atribuídas à Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por estabelecer diretrizes, normas, procedimentos e fiscalizar o tratamento de dados pessoais no Brasil. A ANPD também atua em cooperação com o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que reúne representantes da sociedade civil, do governo e do setor privado para promover o debate e o desenvolvimento de políticas públicas voltadas à proteção de dados (Brasil, 2018).

Segundo Oliveira et al. (2019), quando aplicada ao contexto da Internet das Coisas (IoT), a LGPD enfrenta obstáculos importantes. Muitos dispositivos IoT trabalham de forma autônoma, com capacidade limitada de processamento e sem interfaces claras com os usuários. Isso dificulta a implementação de mecanismos como a coleta de consentimento, a gestão de preferências ou a exclusão de dados pessoais. Esses desafios técnicos colocam em risco a efetividade prática da conformidade legal em ambientes altamente distribuídos e dinâmicos, como os sistemas IoT.

Sendo assim, é fundamental investigar como os princípios e exigências da LGPD podem ser aplicados, ou adaptados, na IoT, e quais soluções têm sido propostas para conciliar inovação tecnológica com responsabilidade jurídica.

3 TRABALHOS RELACIONADOS

Neste capítulo serão apresentados estudos anteriores que tratam de temas relacionados à presente pesquisa, principalmente aqueles que tratam da privacidade na Internet das Coisas (IoT), com a aplicação da Lei Geral de Proteção de Dados (LGPD). Os trabalhos selecionados foram considerados por sua proximidade temática, metodológica ou por contribuírem com bases teóricas relevantes para o desenvolvimento deste trabalho.

3.1 Internet das coisas e privacidade: uma revisão sistemática de literatura

Existem alguns trabalhos que revisam a literatura com o objetivo de identificar aspectos relacionados à privacidade no uso de tecnologias que estão surgindo. Destaca-se o estudo de Oliveira et al. (2018), com a realização de uma revisão sistemática da literatura, analisa como a privacidade tem sido discutida no contexto da Internet das Coisas. Os autores identificam temas que surgem com frequência, como proteção de dados pessoais, comportamento do usuário e aspectos legais, além de diferentes formas de classificar a privacidade.

Portanto, com este estudo temos uma visão geral da produção científica sobre o tema, podendo ser útil tanto para pesquisadores interessados em compreender as abordagens existentes quanto para profissionais que buscam integrar preocupações com privacidade em projetos com IoT. No entanto, como foi publicado antes da entrada em vigor da LGPD, o trabalho não foca diretamente nos desafios de conformidade com a legislação brasileira, o que mostra a relevância da presente pesquisa em complementar e atualizar essa discussão.

3.2 Observabilidade em sistemas de Internet das Coisas: um mapeamento sistemático.

No trabalho de Arantes (2021), foi realizado um mapeamento sistemático sobre a observabilidade em sistemas IoT, com o objetivo de compreender como o monitoramento, rastreamento e análise de comportamento desses sistemas têm sido tratados na literatura. O autor destaca que a observabilidade é fundamental para afirmar que requisitos não funcionais como segurança, disponibilidade e desempenho, principalmente em ambientes com dispositivos diversos e com um alto volume de dados.

Ainda que o foco principal do estudo citado não seja a privacidade ou a LGPD, suas contribuições podem ser relevantes por tratarem de técnicas e desafios técnicos que também impactam a proteção de dados em dispositivos IoT. Sendo assim, o trabalho oferece uma base

complementar para a presente pesquisa, especialmente por adotar a mesma metodologia de mapeamento sistemático e por abordar elementos que se relacionam diretamente com a necessidade de conformidade em sistemas distribuídos.

3.3 A Lei Geral de Proteção de Dados pessoais aplicada à Internet das Coisas: uma revisão sistemática

Alguns estudos exploram os desafios da aplicação da LGPD em ambientes tecnológicos. Podemos destacar o trabalho desenvolvido por Costa (2022), que analisa, por meio de uma revisão sistemática, a relação entre a LGPD e a IoT. O estudo propõe soluções baseadas em modelos de referência já existentes, com o objetivo de garantir a conformidade sem comprometer a funcionalidade dos dispositivos conectados.

A proposta do autor consiste em alinhar práticas existentes às exigências da LGPD, sem propor mudanças estruturais nas tecnologias utilizadas. Por mais que se adote uma abordagem teórica, o estudo tem uma proposta semelhante à presente pesquisa ao discutir a necessidade de adaptação das soluções tecnológicas à legislação brasileira de proteção de dados. O estudo de Costa (2022) se concentra em conceitos normativos e soluções de adequação, oferecendo contribuições para a presente pesquisa, que busca mapear sistematicamente as técnicas discutidas para identificar a conformidade da IoT com a LGPD.

3.4 Dos desafios da implementação da lei geral de proteção de dados no campo de IOT

O artigo apresentado por Motta (2023) apresenta os principais desafios jurídicos relacionados à aplicação da LGPD em dispositivos IoT. A autora destaca a complexidade em garantir o consentimento informado dos usuários, considerando a natureza de maneira independente e muitas vezes invisível com relação a coleta de dados por esses dispositivos. Além do mais, o estudo aborda a dificuldade de identificar os responsáveis pelo tratamento de dados em sistemas IoT, que frequentemente envolvem múltiplos agentes. A pesquisa reforça a necessidade de desenvolver estruturas técnicas e regulações específicas para assegurar a conformidade com a LGPD nesse cenário.

Este trabalho complementa o presente trabalho ao fornecer uma perspectiva jurídica detalhada sobre os desafios com relação à proteção de dados na IoT. O artigo foca nos aspectos legais e regulatórios, a monografia propõe uma abordagem que também considera soluções técnicas com relação à privacidade e a segurança dos dados em dispositivos IoT.

3.5 Internet das Coisas e Big Data na nova Lei de Proteção de Dados: Análise da proteção dos dados sensíveis

O trabalho de Cavalcanti (2022), desenvolvido na Faculdade de Direito de Vitória, aborda os desafios legais da proteção de dados sensíveis diante do uso combinado da IoT e tecnologias de big data. A autora contextualiza os riscos relacionados à coleta intensa e muitas vezes invisível de informações por dispositivos conectados e discute como a LGPD pode (ou não) oferecer maneiras eficazes de proteção. Sua análise prioriza os obstáculos técnicos e regulatórios que dificultam a conformidade com a legislação, em especial no que se refere à exigência de consentimento e à tutela dos direitos dos titulares.

O foco da autora está voltado à análise teórica e normativa, o seu estudo oferece uma visão valiosa sobre as implicações legais da coleta de dados. A presente pesquisa complementa esse trabalho ao propor uma análise sistemática das abordagens técnicas publicadas na literatura científica, buscando identificar como a conformidade com a LGPD tem sido tratada em soluções para IoT.

3.6 Considerações finais sobre os trabalhos relacionados

Os estudos analisados apresentam contribuições relevantes para a compreensão dos desafios de privacidade e conformidade legal no contexto da Internet das Coisas, principalmente em relação à aplicação da LGPD. No entanto, é notório que muitos deles possuem focos específicos, como a discussão jurídica, abordagens normativas ou revisões teóricas, que por mais importante que seja, limita a visão prática e técnica sobre a implementação da conformidade em dispositivos IoT. Além disso, a maioria dos trabalhos utiliza revisões de literatura ou análises conceituais, sem realizar um resumo sistemático das abordagens técnicas que vêm sendo propostas ou adotadas na literatura científica.

Diante disso, o presente trabalho busca preencher essa lacuna ao realizar um mapeamento sistemático mostrando as abordagens técnicas e metodológicas discutidas na literatura que tratam da privacidade em dispositivos IoT sob a ótica da conformidade com a LGPD. Ao integrar diferentes abordagens, técnicas, jurídicas e operacionais, esta investigação pretende oferecer uma contribuição ao identificar padrões, desafios recorrentes e soluções práticas já existentes.

Os elementos comparativos estão contidos na Tabela 1.

Tabela 1 – Comparação dos Trabalhos Relacionados

Trabalho	Contribuições	Influência na presente pesquisa
Internet das coisas e privacidade: uma revisão sistemática de literatura	Identifica temas recorrentes como proteção de dados e aspectos legais, apresentando diferentes formas de classificar privacidade	Serviu de base para compreender de forma geral sobre privacidade em IoT
Observabilidade em sistemas de Internet das Coisas: um mapeamento sistemático	Destaca importância de monitoramento e rastreamento, aponta desafios técnicos em ambientes distribuídos	Influenciou na estruturação da metodologia de um mapeamento sistemático na presente pesquisa
A Lei Geral de Proteção de Dados pessoais aplicada à Internet das Coisas: uma revisão sistemática	Apresenta soluções baseadas em modelos de referência e propõe adequações sem mudanças estruturais	Ajudou na análise da relação entre soluções técnicas e exigências da LGPD
Dos desafios da implementação da lei geral de proteção de dados no campo de IOT	Identifica desafios jurídicos como consentimento e identificação de agentes	Ajudou a entender como é os desafios jurídicos no campo da IoT
Internet das Coisas e Big Data na nova Lei de Proteção de Dados: Análise da proteção dos dados sensíveis	Discute riscos e obstáculos técnicos/regulatórios e foca em consentimento e direitos dos titulares	Contribuiu para entender melhor sobre dados sensíveis e Big Data na IoT

Fonte: Autoria Própria (2025)

4 METODOLOGIA

Esta pesquisa adota a abordagem de Mapeamento Sistemático da Literatura a partir das diretrizes propostas por Petersen et al. (2008). Esse estudo apresenta um ponto de vista de uma área de pesquisa, categorizando e quantificando a produção científica existente, permitindo o reconhecimento de lacunas, tendências e concentrações de esforços na literatura.

4.1 Planejamento do mapeamento sistemático

Nesta fase, será elaborado um protocolo contendo as questões que guiará a categorização e a análise dos estudos, os critérios de inclusão e exclusão, as bases de dados a serem utilizadas, a string de busca e o plano de extração de dados. As perguntas desta pesquisa são:

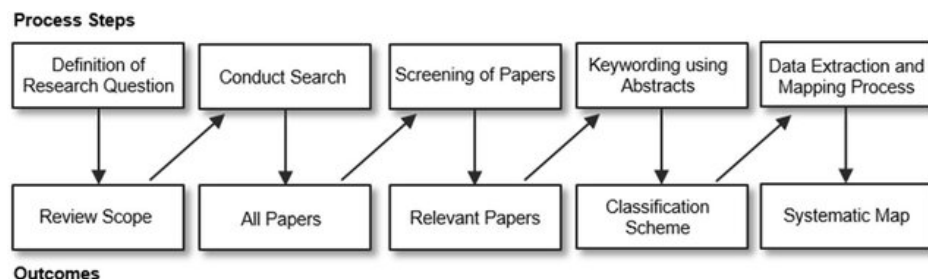
- Q1. Quais são as abordagens propostas para garantir a conformidade com a LGPD em dispositivos IoT?
- Q2. Em quais contextos os dispositivos IoT são aplicados nos estudos que abordam LGPD?
- Q3. Quais desafios são apontados para a aplicação da LGPD em IoT?
- QA1: Quais são os tipos dos trabalhos científicos publicados?
- QA2: Como o número de publicações é distribuído ao longo dos anos?
- QA3: Quais são os locais de filiação dos autores?

Essas perguntas ajudaram na estrutura de extração dos dados quanto na classificação utilizada dos resultados.

4.2 Condução do mapeamento sistemático

O processo de condução do mapeamento sistemático seguiu as etapas essenciais propostas por Petersen et al. (2008), conforme ilustrado na Figura 1.

Figura 1 - O Processo de Mapeamento Sistemático



Fonte: Petersen et al. (2008)

Para apoiar as fases de triagem, extração e organização dos estudos, foram utilizadas

planilhas elaboradas especificamente para gerenciar as strings de busca, aplicar os critérios de inclusão e exclusão e registrar, de forma estruturada, as informações extraídas. Esse recurso contribui para um maior controle metodológico durante todo o processo de revisão.

A condução do estudo contemplou as seguintes etapas:

- Busca dos estudos primários: Utilização de uma string de busca estruturada, aplicada em bases como IEEE Xplore, Scopus, ACM Digital Library, Oasisbr. A string será composta por termos-chave relacionados a “LGPD”, “IoT”. Considerando a presença de publicações em diferentes idiomas, serão desenvolvidas versões da string em português e em inglês, de forma que aumente a cobertura dos estudos que sejam relevantes.
- Triagem dos estudos: Aplicação dos critérios de inclusão e exclusão, com triagem por título, resumo e leitura completa. Serão excluídos artigos que não tratam diretamente da conformidade com a LGPD em dispositivos IoT, artigos duplicados, livros, resumos expandidos.
- Keywording dos resumos: Os resumos dos artigos selecionados serão analisados para extrair palavras-chave e conceitos, que servirão de base para a construção do esquema de classificação.
- Extração e mapeamento dos dados: Cada artigo será classificado de acordo com as características identificadas, tais como: tipo de abordagem, tipo de pesquisa (sugestões de solução, pesquisa de validação e avaliação, artigo etc.), e foco da LGPD.

Cada etapa produz um resultado, que conduz ao próximo passo do processo: definição do escopo do mapeamento, conjunto inicial de artigos, conjunto filtrado de estudos relevantes, esquema de classificação e, por fim, o mapa sistemático como produto final. Essa abordagem garante que a revisão seja conduzida de maneira estruturada, transparente e reaplicável, proporcionando uma visão abrangente e confiável sobre o tema investigado.

4.3 Síntese do processo metodológico

No presente estudo, a síntese seguirá uma abordagem baseada em conjuntos definidos primeiramente no protocolo de pesquisa. Serão analisadas tanto informações quantitativas, como frequência de publicações e tipos de abordagem, quanto aspectos qualitativos, como o conteúdo das propostas identificadas. A apresentação dos resultados será realizada por meio de tabelas com as principais facetas adotadas, e gráficos, com o intuito de proporcionar uma visão clara e organizada da pesquisa sobre conformidade com a LGPD em dispositivos IoT. A

apresentação dos dados seguirá os padrões recomendados por Petersen et al. (2008), permitindo uma visão estruturada das tendências e lacunas da literatura científica.

5 RESULTADOS

O presente capítulo visa apresentar os resultados obtidos por meio do Mapeamento Sistemático da Literatura (MSL) realizado. Inicialmente, são apresentadas as perguntas de pesquisa que conduziram o estudo (Seção 5.1), seguidas pela construção da string de busca (Seção 5.2) e pela definição das bases de dados selecionadas para a coleta dos estudos (Seção 5.3). Na sequência, são apresentados os critérios de inclusão e exclusão (Seção 5.4) e o processo de triagem dos estudos (Seção 5.5), detalhando a quantidade de artigos em cada etapa até a seleção final. Em seguida, é apresentado o esquema de classificação e extração dos dados (Seção 5.6), no qual foram organizadas as principais facetas adotadas, como abordagens, áreas de aplicação e desafios. A análise visual e descritiva dessas facetas é realizada na Seção 5.7, por meio de gráficos e discussões. Por fim, a Seção 5.8 apresenta as respostas às perguntas de pesquisa propostas, com base nos resultados extraídos e categorizados.

5.1 Questões da pesquisa

Para facilitar a análise dos estudos selecionados e garantir que os objetivos do mapeamento sistemático sejam atendidos, foram elaboradas questões de pesquisa e questões adicionais que darão sentido à extração e à organização dos dados. Para o presente trabalho, o mapeamento sistemático contém as seguintes questões principais de pesquisa:

Q1: Quais são as abordagens propostas para garantir a conformidade com a LGPD em dispositivos IoT?

Q2: Em quais contextos os dispositivos IoT são aplicados nos estudos que abordam LGPD?

Q3: Quais desafios são apontados para a aplicação da LGPD em IoT?

Além disso, foram formuladas três questões adicionais para caracterização dos estudos:

QA1: Quais são os tipos dos trabalhos científicos publicados?

QA2: Como o número de publicações é distribuído ao longo dos anos?

QA3: Quais são os locais de filiação dos autores?

5.2 String de buscas

As *strings* de busca, foram elaboradas com a intenção de oferecer uma busca eficiente e precisa dentro de cada base, foi escolhida para abranger diferentes variações e traduções dos

termos relevantes ao tema abordagens de privacidade em dispositivos IoT com conformidade da LGPD. O intuito era aumentar o nível de relevância dos artigos encontrados, para a inclusão de fontes tanto em inglês quanto em português, para assegurar uma coleta ampla.

A *string* de busca utilizada foi:

- ***("IoT" OR "Internet das Coisas" OR "Internet of Things") AND ("LGPD" OR "Lei Geral de Proteção de Dados" OR "General Data Protection Law")***

A string foi escolhida com o intuito de coletar artigos que abordassem de forma direta a privacidade dos dispositivos IoT, para entender o contexto dos dispositivos e como se tratava suas privacidades e coletar informações sobre a LGPD, para assim identificar suas lacunas com relação aos dispositivos IoT. A utilização do operador "AND" certifica que ambos os termos estejam sendo abordados na presente coleta, filtrando resultados mais específicos para o tema. E o termo "OR" é utilizado para que se um dos termos não for encontrado, tentar por outro termo, seja ele em português ou inglês.

5.3 Bases de artigos para pesquisa

Para a coleta de artigos, foi necessária a utilização de algumas bases de pesquisa, para garantir uma apresentação relevante para o estudo. As bases selecionadas para a coleta foram as seguintes: IEEE Xplore, ACM Digital Library, Oasisbr, Scopus. A coleta desses dados foram feitas manualmente nas plataformas selecionadas com a utilização de planilhas, que ajudaram na organização, com os resultados apresentados cobrindo um período de 2019 até 2024. A quantidade exata de cada artigo encontrado será exposta na Tabela 2 abaixo.

Tabela 2 – Documentos retornados por base de busca

Bases de Pesquisa	Resultados
IEEE Xplore	2
ACM Digital Library	32
Oasisbr	42
Scopus	120
Total:	196

Fonte: Autoria própria (2025)

5.4 Critérios de inclusão e exclusão

Além disso, foram estabelecidos critérios de inclusão e exclusão dos artigos, para se assegurar que somente os estudos mais relacionados e compatíveis com os objetivos da pesquisa fossem selecionados.

5.3.1 Critérios de inclusão

- **O estudo aborda a Lei Geral de Proteção de Dados (LGPD) aplicada a dispositivos ou sistemas IoT (Internet das Coisas).**

Este critério assegura que o foco do estudo envolva a aplicação da LGPD no contexto da IoT, garantindo a ligação ao tema proposto da pesquisa

- **Aborda diretamente questões ou desafios relacionados à privacidade, proteção de dados ou conformidade legal em dispositivos IoT.**

Estudos que exploram aspectos práticos ou teóricos da privacidade e segurança de dados em IoT são incluídos.

- **Menciona explicitamente a LGPD (Lei Geral de Proteção de Dados)**

Esse critério busca garantir que os estudos considerados esteja relacionado com as normas de proteção de dados.

- **Foi publicado entre 2019 e 2024, período correspondente à entrada em vigor da LGPD e aos anos seguintes.**

Esse intervalo é relevante para garantir que os estudos mostrem discussões atuais e compatíveis com a vigência da legislação.

- **Está disponível em texto completo para leitura e análise.**

Este critério assegura que os artigos possam ser examinados totalmente para extração e categorização de dados.

5.3.2 Critérios de exclusão

- **O conteúdo não faz qualquer relação entre LGPD e IoT, ou trata dos temas de forma completamente desvinculada do foco da pesquisa.**

São excluídos os estudos que mencionam os temas apenas superficialmente ou em contextos diferentes do tema.

- **O documento é um trabalho de conclusão de curso (TCC), resumo expandido, tutorial, short paper ou apresentação de workshop, livros, slides.**

O foco da pesquisa está em artigos científicos, teses ou dissertações completas que

tenham passado por avaliação e apresentam estrutura formal.

- **O estudo é um trabalho secundário, como uma Revisão Sistemática da Literatura (RSL) ou outro Mapeamento Sistemático.**

A pesquisa busca apenas estudos primários, ou seja, que apresentem dados originais ou propostas relacionadas à temática.

5.5 Desenvolvimento do mapeamento sistemático

Nesse sentido, após a conclusão da Fase 1, que se tratou da coleta de artigos com base na leitura de títulos, resumos e identificação de palavras-chave, foram identificados 196 artigos. Desses, 158 foram excluídos ainda na Fase 1, com base nos critérios de inclusão e exclusão definidos. Resultando assim, 38 artigos que avançaram para a Fase 2, que consistiu na leitura de títulos, resumos, palavras-chave, introdução e conclusão, além de realizar a aplicação dos critérios de inclusão e exclusão descritos. Ao término da Fase 2, 15 artigos foram excluídos, resultando em 23 artigos selecionados para a fase final, que consistirá em entender melhor cada documento. A quantidade de artigos que avançaram para a Fase 2 são apresentados na Tabela 3.

Tabela 3 – Resultado dos documentos retornados na Fase 2

Base de Pesquisa	Artigos avançados na Fase 2
IEEE Xplore	2
ACM Digital Library	4
Oasisbr	19
Scopus	13
Total	38

Fonte: Autoria própria (2025)

Após a conclusão da Fase 2, que resultou em 38 artigos, foi dado início a fase final, que inclui a leitura completa dos textos. Como resultado, foram incluídos 23 artigos e excluídos 15, totalizando 23 artigos no final do processo. A quantidade será exposta abaixo na Tabela 4.

Tabela 4 – Resultado dos documentos retornados na Fase Final

Base de Pesquisa	Incluídos	Excluídos
IEEE Xplore	2	0
ACM Digital Library	1	3
Oasisbr	12	7
Scopus	8	5
Total	23	15

Fonte: Autoria própria (2025)

5.6 Esquema de classificação e extração dos dados

Abaixo, destaca-se uma Tabela com os artigos analisados e aceitos para compor o presente mapeamento sistemático, no qual o foco é investigar as abordagens de privacidade em dispositivos da IoT sob a ótica da conformidade com a LGPD.

A seleção dos artigos foi feita com base nos critérios de inclusão e exclusão definidos na Seção 5.4, levando em consideração a relevância das obras no contexto da proteção de dados em ambientes IoT. Os documentos foram obtidos em bases acadêmicas reconhecidas já citadas, cobrindo o período de 2018 a 2025.

Para cada estudo, são apresentados: um identificador único (ID), o título do trabalho, a referência, e uma breve descrição do conteúdo, destacando os objetivos. Essa estruturação visa proporcionar uma visão clara e organizada da literatura analisada, facilitando a extração e a categorização dos dados nas etapas seguintes do mapeamento, especialmente na elaboração das respostas às perguntas de pesquisa.

Tabela 5 - Análise dos estudos aprovados.

ID	Título	Referência (ABNT)	Descrição
1	Brazilian scenarios for smart cities deployment from public policies perspectives	(Bernardi, E. et al., 2020)	O artigo relata algumas regulamentações técnicas e políticas brasileiras e internacionais com relação a cidades inteligentes, com foco na LGPD e políticas públicas.
2	Securing Data at Rest: Using ML-Driven Personally Identifiable Information (PII) Detection and Privacy-Preserving Techniques	(Nadella, D., 2024)	O artigo propõe um framework baseado em aprendizado de máquina e técnicas de preservação de privacidade para detectar e proteger PII armazenado em repouso.
3	A Blockchain-Based Privacy-Preserving Model for Consent and Transparency in Human-Centered Internet of Things	(Jorge Eduardo Rivadeneira et al., 2023)	Propõe um modelo de preservação da privacidade baseado em blockchain para gerenciamento de consentimento e transparência em sistemas IoT centrados no humano
4	Evolution and regulation of privacy and data protection in the context of the internet of things in the brazilian scenario	(Calaza, T., 2024)	Faz uma análise sobre a evolução histórica das regulamentações de privacidade e proteção de dados no Brasil e no cenário internacional, destacando sua relação com a IoT.
5	Privacy protection under the general data protection law (lgpd) in the era of the internet of things (iot)	(Bianchi, D.; Consalter, G., 2024)	Analisa se os mecanismos previstos pela LGPD são suficientes para proteger os dados pessoais e sensíveis dos usuários diante do crescimento da IoT
6	Handling of Personal Data by Smart Home Equipment: an Exploratory Analysis in the Context of LGPD	(Coleti, T. A. et al., 2024)	Investigar quais dados pessoais são de maior interesse por equipamentos de smart home e verificar se esses dispositivos estão em conformidade com os requisitos de transparência estabelecidos pela LGPD.

(continua)

Tabela 5 - Análise dos estudos aprovados (continuação).

7	Digital Platform for Continuous Monitoring of Patients Using a Smartwatch: Longitudinal Prospective Cohort Study	(Bin, K. J. et al., 2023)	Desenvolver e validar um modelo funcional para captura de dados de smartwatch e envio à anonimização de serviços de saúde, respeitando a legislação, para uso clínico durante o monitoramento remoto de pacientes.
8	Internet of things (IoT) and citizens' rights to privacy and data protection: a necessary approach	(Limberger, t.; Da, g.; Giannakos, s., 2024)	Refletir sobre os impactos da IoT nos direitos fundamentais à privacidade e à proteção de dados, abordando a necessidade de conformidade legal diante do avanço da Indústria 4.0 e da coleta de informações pessoais.
9	A case study on the development of a data privacy management solution based on patient information	(Verri Lucca, A. et al., 2020)	Desenvolver uma solução de gestão de privacidade baseada em uma taxonomia aplicada a ambientes hospitalares, com foco em pacientes suspeitos de COVID-19, visando garantir segurança e anonimato no manuseio de dados sensíveis.
10	Facial recognition in smart cities and the guarantee of the rights to privacy and personal data protection	(Dal Magro, D.; Fortes, V. B., 2021)	Investigar como o modelo chinês de reconhecimento facial em smart cities impacta os direitos fundamentais à privacidade e proteção de dados pessoais no Brasil.
11	The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy	(Fornasier, M. D. O., 2019)	Analisar como a aplicação do IoT à área da saúde pode afetar os direitos fundamentais à saúde e à privacidade, considerando aspectos legais, éticos e de segurança da informação, com foco na realidade brasileira.
12	Governança e privacidade de dados pessoais: estudo de caso dos usuários de veículos conectados na perspectiva da indústria à luz da Lei Geral de Proteção de Dados Brasileira (LGPD)	(Carvalho da silva, Nivaldo., 2021)	Propor um modelo de governança da informação e da privacidade de dados pessoais no contexto de veículos conectados, considerando os princípios da LGPD e os desafios regulatórios.

Tabela 5 - Análise dos estudos aprovados (continuação).

13	Estendendo um checklist de inspeção da aderência de soluções à LGPD para avaliar critérios específicos de IoT	(Gomes Neto, Ivonildo Pereira., 2022.)	Propor um checklist de inspeção estendido para verificar a conformidade de projetos envolvendo dispositivos IoT com a LGPD, considerando as características específicas desses dispositivos e suas implicações na proteção de dados.
14	A privacidade está on? Uma avaliação nos textos de políticas de privacidade e termos de uso de artefatos IoT em relação à lei geral de proteção de dados	(Zeferino, André Ferreira., 2021)	Avaliar a conformidade das Políticas de Privacidade e Termos de Uso de dispositivos IoT com a LGPD, utilizando análise computacional de similaridade textual.
15	Abordagem IoT PD-RPM: Promovendo Aderência à Diálise Peritoneal Considerando o Cenário da Internet das Coisas	(Alblandes, Rogério Da Costa., 2024)	Desenvolver uma abordagem baseada em IoT para promover o apoio de pacientes e profissionais de saúde à diálise peritoneal domiciliar, assegurando o monitoramento remoto com respeito às diretrizes da LGPD.
16	Direito Digital na era da internet das coisas: o direito à privacidade e a Lei Geral de Proteção de Dados Pessoais = Digital Law in the IoT age: the right to privacy and the Law of Protection of Personal Data	(Castro, Bárbara Brito de. 2019)	Analisar os impactos jurídicos da IoT sobre o direito à privacidade e à proteção de dados pessoais, à luz do Direito Eletrônico e da LGPD, destacando a necessidade de evolução diante da nova realidade tecnológica.
17	Coleta, utilização indevida e proteção de dados no ambiente digital na legislação brasileira: a internet das coisas como sistema de transferência de dados pessoais	(Cruz, Eduardo Otaciano da. 2024)	Explorar os desafios legais e regulatórios com a privacidade e à proteção de dados no contexto da IoT, com foco na legislação brasileira, especialmente a LGPD, frente à coleta, processamento e uso indevido de dados pessoais gerados por dispositivos conectados.
18	(Des) proteção de dados e internet das coisas: os desafios à tutela dos dados de saúde de usuários de dispositivos de IOT à luz dos preceitos da LGPD	(Ruviano, Eduardo Missau. 2021)	Investigar como a LGPD pode contribuir, de forma preventiva ou reparadora, para a proteção dos dados pessoais sensíveis de saúde dos usuários de aplicações conectadas à IoT.

Tabela 5 - Análise dos estudos aprovados (conclusão).

19	Internet das coisas e responsabilidade civil : os riscos do desenvolvimento dos dispositivo	(Roncatto, carolina da rosa. 2022)	Analisar os impactos da IoT no Direito Civil brasileiro, no campo da responsabilidade civil, para compreender como o ordenamento jurídico pode lidar com os novos riscos e danos provocados por dispositivos conectados.
20	Modelo de captura de dados por internet das coisas e disponibilização dos mesmos para uso clínico e de pesquisa seguindo as leis de proteção de dados	(Bin, Kaio Jia. 2023)	Apresentar e validar um modelo funcional de captura de dados clínicos via dispositivos IoT, e a disponibilização desses dados para uso clínico e em pesquisa médica, garantindo conformidade com a LGPD.
21	Internet of Things and blockchain used in the Brazilian Unified Health System: how to protect sensitive data considering the imminence of the Data Protection Law	(Câmara, M. A. A. et al. 2021)	Analisar as fragilidades na proteção da privacidade dos usuários do SUS frente ao uso crescente de tecnologias IoT e propor uma solução teórica baseada em personal data stores (PDS) e blockchain para garantir maior segurança dos dados sensíveis, com a aplicação da LGPD
22	Segurança da informação e proteção de dados pessoais: estudo de caso e proposta de governança para serviços de saúde.	(Silveira, S. A. 2021.)	Apresentar uma análise dos riscos, e desafios da segurança da informação e proteção de dados pessoais no setor de saúde, em serviços de e-saúde, e propor uma abordagem de governança para proteger a confidencialidade, integridade e disponibilidade das informações dos pacientes.
23	Nova privacidade no Brasil e os impactos jurídicos e econômicos: uma análise do big data e da responsabilidade empresarial	(Lannes, Yuri Nathan da Costa. 2020.)	O estudo visa compreender como as novas tecnologias afetam a privacidade e quais os limites jurídicos e institucionais existentes, destacando o papel do Estado na regulamentação e proteção dos dados pessoais.

Fonte: Autoria Própria (2025)

As abordagens que foram encontradas nos estudos entre os anos de 2019 a 2024, foram organizadas em sete dimensões principais, com o intuito de estruturar as diferentes abordagens adotadas para tratar da privacidade em dispositivos IoT sob a ótica da LGPD. A dimensão Jurídico abrange estudos que analisam diretamente a LGPD, com foco em princípios legais e implicações jurídicas do tratamento de dados pessoais. A dimensão Anonimização reúne estudos que propõem ou discutem técnicas específicas para anonimizar dados, visando minimizar os riscos à privacidade. A categoria Machine Learning são trabalhos que aplicam algoritmos de aprendizado de máquina para detectar dados sensíveis, identificar padrões de uso ou oferecer proteção automatizada. Já a dimensão de Avaliação de Conformidade refere-se a estudos que propõem metodologias, indicadores ou processos formais para verificar o uso de sistemas e dispositivos IoT às exigências da LGPD.

Logo mais, a dimensão Checklist trata de estudos que propõem listas de verificação estruturadas como instrumentos de diagnóstico ou adequação à legislação. A dimensão Blockchain contempla abordagens que utilizam essa tecnologia como meio de garantir transparência, rastreabilidade e controle sobre o uso e o compartilhamento de dados pessoais. E por fim, a dimensão Governança refere-se a propostas voltadas à implementação de boas práticas institucionais, modelos organizacionais e políticas internas voltadas à gestão da privacidade e da segurança da informação.

A Tabela contendo a Faceta que detalha as abordagens apresenta a distribuição dos estudos conforme essas dimensões, e corresponde à pergunta elaborada da questão **Q1**.

Tabela 6 - Faceta: Abordagens

Dimensão	Referência (ID)
Jurídico	1; 4; 5; 8; 10; 11; 16; 17; 18; 19; 23.
Anonimização	7; 9; 20.
Machine Learning	2.
Avaliação de Conformidade	6; 14; 15.
Checklist	13.
Blockchain	3; 21.
Governança	12; 22.

Fonte: Autoria própria (2025)

Foi realizada também a análise das aplicações dos dispositivos IoT nos estudos incluídos no mapeamento sistemático que permitiu identificar os principais contextos em que essas tecnologias são aplicadas em conformidade com a LGPD. Os contextos foram reunidos em seis dimensões de aplicação: Saúde, Cidades Inteligentes, Smart Home, Veículos Conectados e Geral.

A organização dessas aplicações em dimensões permite compreender como os dispositivos IoT têm sido utilizados na prática e em quais setores a conformidade com a LGPD tem sido mais explorada ou abordada.

A Tabela a seguir apresenta a distribuição dos artigos conforme essas dimensões, e corresponde à pergunta elaborada da questão **Q2**.

Tabela 7 - Faceta: Aplicações referentes aos estudos analisados

Dimensão	Referência
Saúde	3; 7; 9; 11; 15; 18; 21; 20; 22.
Cidades Inteligentes	1; 3; 10.
Veículos Conectados	12.
Smart Home	6.
Geral	2; 4; 5; 8; 13; 14; 16; 17; 19; 23.

Fonte: Autoria própria (2025)

A Faceta a seguir tem como objetivo identificar os desafios mais pertinentes e discutidos nos estudos analisados quanto aos dispositivos IoT no contexto da Lei Geral de Proteção de Dados (LGPD).

A Faceta apresenta a distribuição dos artigos conforme os desafios identificados, permitindo visualizar de forma clara quais aspectos são mais frequentes na literatura sobre o tema. Essa categorização contribui para destacar os pontos críticos que merecem maior atenção em pesquisas futuras, bem como para orientar estratégias de conformidade mais eficazes em uso da IoT.

A Tabela a seguir apresenta a distribuição dos artigos conforme essas dimensões, e corresponde à pergunta elaborada da questão **Q3**.

Tabela 8 - Faceta: Desafios enfrentados nos estudos

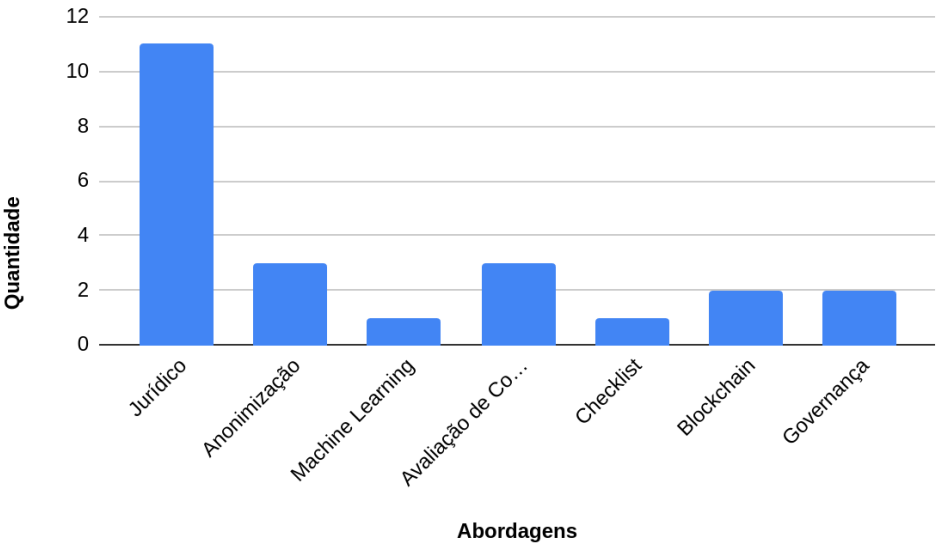
Dimensão	Referência
Consentimento	3; 6; 8; 10; 11; 12; 14; 17; 18; 19; 21.
Limitações técnicas	3; 9; 13; 14; 15; 20; 21; 22.
Segurança na proteção de dados	2; 5; 7; 9; 11; 12; 13; 15; 18; 19; 20; 21; 22.
Regulamentações	1; 4; 5; 6; 8; 10; 11; 12; 13; 14; 16; 17; 18; 19; 20; 21; 22; 23.

Fonte: Autoria própria (2025)

5.7 Análise das respostas

Para facilitar a análise dos estudos incluídos no mapeamento sistemático, foram elaborados dois gráficos de barras, representando visualmente a distribuição das publicações conforme as abordagens propostas e os contextos de aplicação dos dispositivos IoT relacionados à conformidade com a LGPD.

Gráfico 1 – Abordagens Propostas nos Estudos



Fonte: Autoria própria (2025)

O Gráfico 1 apresenta os estudos com base nas categorias de abordagem identificadas: Jurídico, Anonimização, Machine Learning, Avaliação de Conformidade, Checklist,

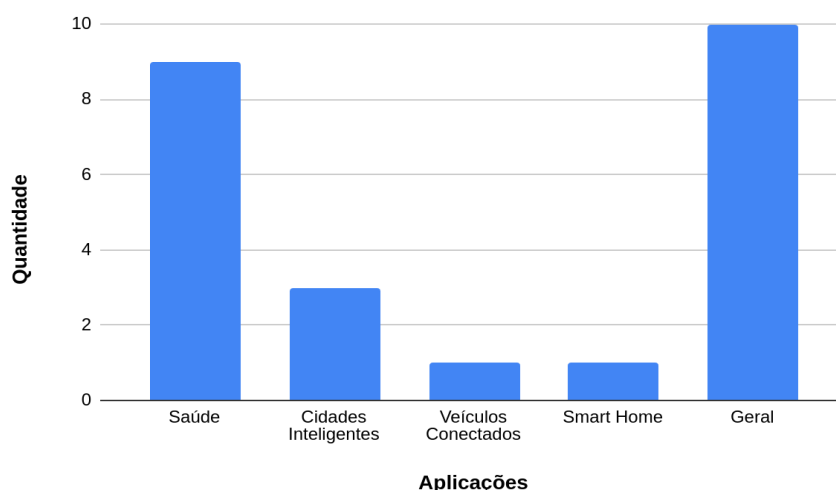
Blockchain e Governança. Essa categorização ajuda a compreender os diferentes focos adotados ao tratar da privacidade e proteção de dados em dispositivos IoT.

A categoria Jurídico foi a mais representada, mostrando a preocupação com a análise da LGPD e demais normativas no contexto de dispositivos conectados. Em seguida, destacam-se os estudos que propõem abordagens como anonimização, voltadas à proteção de dados sensíveis. Abordagens que tratam de blockchain, e estudo que propõe Machine Learning embora que as tecnologias tenham aparecido em menor número ainda assim representam tecnologias emergentes com grande potencial de crescimento. Destaca-se também a categoria de Governança, indicando iniciativas voltadas à estruturação de boas práticas organizacionais e revisões mais amplas da literatura. Por fim, abordagens como avaliação de conformidade e o uso de checklists foram apresentados, ainda que com menor número de estudos.

No Gráfico 2 representa os contextos de aplicação dos dispositivos IoT nos estudos analisados. As aplicações foram agrupadas em seis principais dimensões: Saúde, Cidades Inteligentes, Geral, Smart Home, Veículos Conectados.

O destaque foi para a área da saúde, com maior número de estudos abordando dispositivos vestíveis e tecnologias de e-saúde. Cidades inteligentes também foram um foco importante, enquanto as aplicações em smart homes e veículos conectados foram limitadas, mas revelam o potencial de crescimento da pesquisa. Alguns estudos adotaram uma perspectiva mais ampla e genérica, tratando os dispositivos IoT de forma geral. Esses trabalhos focaram nas questões de privacidade e conformidade à LGPD de maneira ampla, sem delimitar uma aplicação específica.

Gráfico 2 – Aplicações encontradas nos estudos analisados



Fonte: Autoria própria (2025)

O Gráfico 3 abaixo, apresenta a distribuição dos principais desafios identificados nos 23 estudos selecionados no mapeamento sistemático. Os desafios foram agrupados em quatro: Consentimento, Limitações técnicas, Segurança na proteção de dados e Regulamentações.

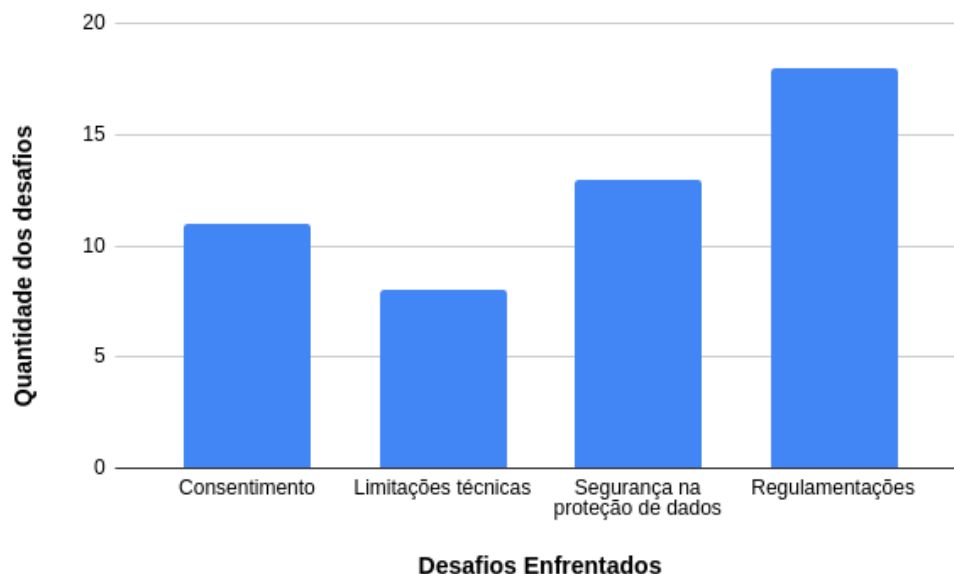
É importante destacar que um mesmo estudo pode ter apontado mais de um desafio, o que justifica o total de ocorrências ser maior que os 23. Esse crescente número mostra como o tema é complexo e como os obstáculos encontrados na hora de cumprir a LGPD em dispositivos IoT estão todos interligados.

O desafio mais recorrente foi Regulamentações, mencionado em 18 estudos, o que indica uma preocupação significativa da literatura com a dificuldade de aplicar de forma efetiva a LGPD em ambientes com dispositivos IoT. Em segundo lugar, o desafio relacionado à Segurança na proteção de dados apareceu em 13 estudos, demonstrando que aspectos como criptografia, proteção contra ataques cibernéticos e falhas de infraestrutura ainda são barreiras relevantes para a garantia da privacidade.

O Consentimento, aspecto central na LGPD, foi identificado como desafio em 11 estudos, destacando desafios na forma como os dados são coletados e como os titulares são informados e participam do processo de tratamento. Já as Limitações técnicas, como barreiras estruturais, ausência de padrões interoperáveis e dificuldades de integração de soluções de privacidade aos dispositivos IoT, foram mencionadas em 8 estudos, embora menos citadas, ainda representam um entrave relevante à conformidade legal e à aplicação prática de mecanismos de proteção.

A análise desses desafios, ajuda a compreender onde estão os principais focos de tensão entre a teoria e a prática na aplicação da LGPD aos sistemas da Internet das Coisas. Esses dados contribuem para orientar futuras pesquisas e intervenções no sentido de superar os obstáculos identificados pela literatura.

Gráfico 3 – Desafios encontrados nos estudos analisados

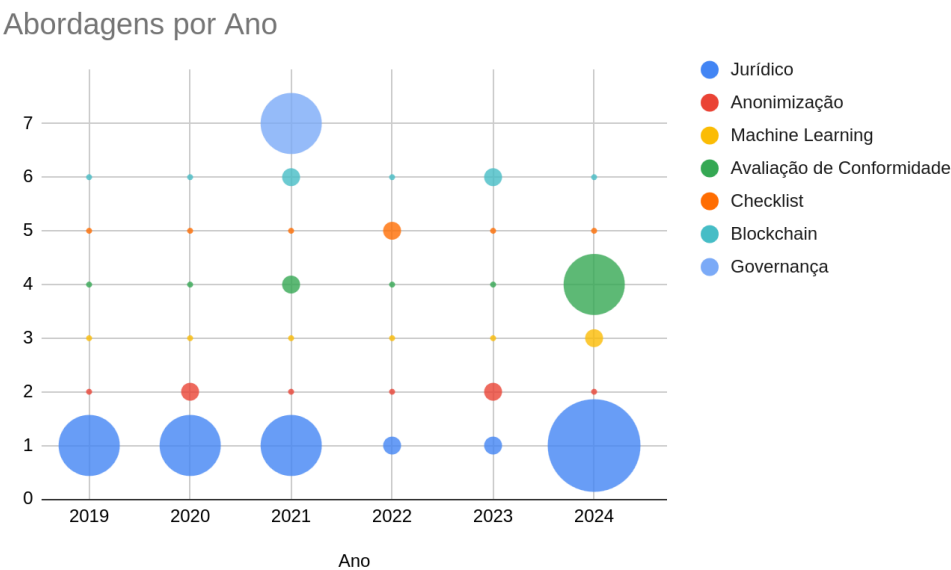


Fonte: Autoria própria (2025)

Para aprofundar a análise da distribuição das abordagens ao longo do tempo, foi elaborado um gráfico de bolhas que correlaciona as dimensões de abordagem identificadas com os anos de publicação dos estudos incluídos no mapeamento sistemático. Cada bolha representa uma ou mais ocorrências de determinada abordagem em um ano específico, e o tamanho da bolha é proporcional à frequência de estudos que utilizam aquela abordagem naquele respectivo ano.

O Gráfico 4 permite visualizar não apenas quais abordagens têm sido mais exploradas, mas também como elas evoluíram ao longo do tempo, mostrando, por exemplo, o surgimento mais recente de técnicas baseadas em *machine learning* ou *blockchain*, como também a constância de abordagens jurídicos em diferentes períodos. A correlação visual entre abordagem ajuda na identificação e compreensão dos caminhos percorridos pela pesquisa sobre privacidade e IoT sob a ótica da LGPD.

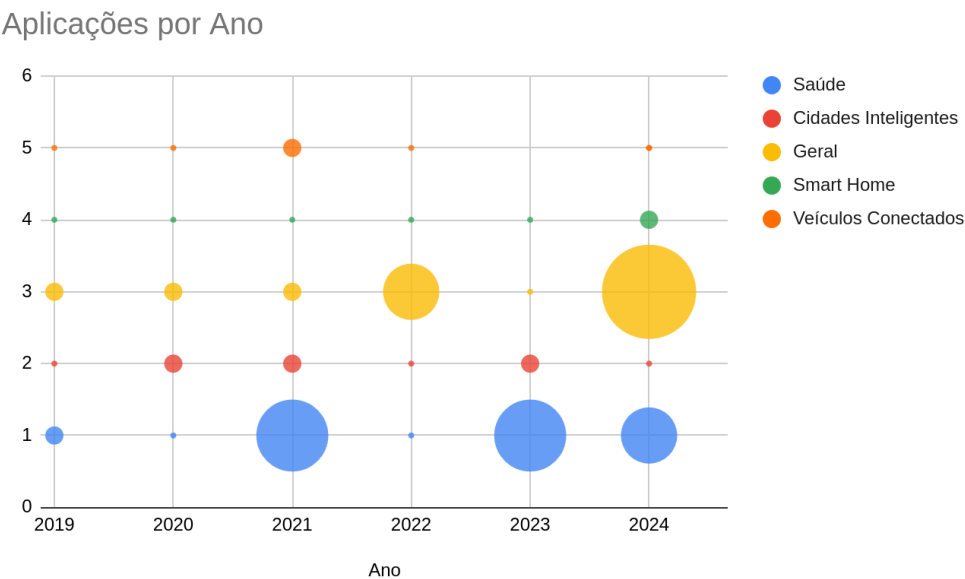
Gráfico 4 – Abordagens exploradas ao longo dos anos



Fonte: Autoria própria (2025)

No Gráfico 5 desenvolvido, está relacionando os anos de publicação com as áreas de aplicação identificadas nos estudos analisados onde é possível observar em que períodos certas aplicações ganharam mais destaque. Essa visualização facilita a identificação de interesse, como o crescimento do interesse por dispositivos IoT em contextos gerais, especialmente em 2024, embora a área da saúde também tenha mantido destaque ao longo dos anos, ou o surgimento de aplicações urbanas e veiculares em momentos específicos.

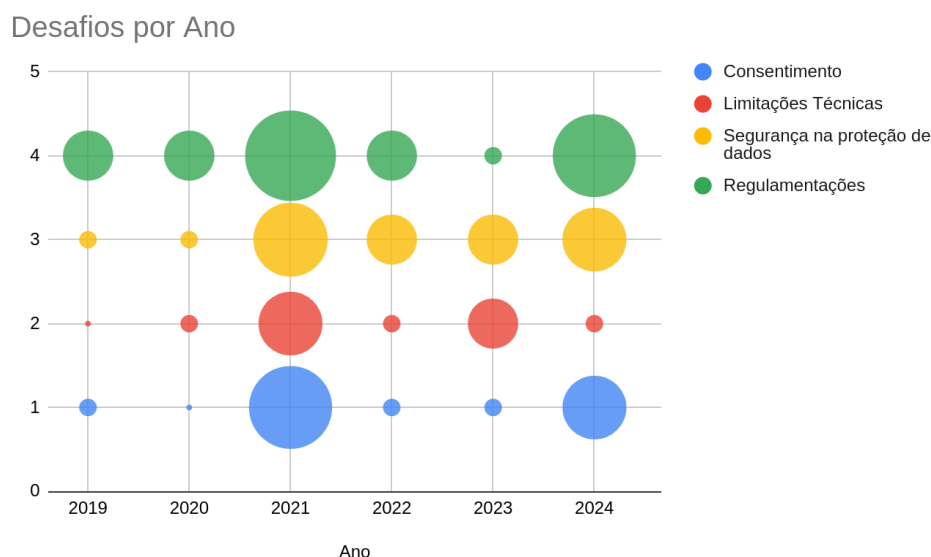
Gráfico 5 – Aplicações exploradas ao longo dos anos



Fonte: Autoria própria (2025)

Temos também o Gráfico 6 que correlaciona os desafios mais recorrentes identificados nos artigos com os anos de publicação. Neste gráfico, cada bolha representa a presença de um desafio específico em determinado ano. É possível identificar, por exemplo, que o desafio da regulamentação se destacou fortemente em 2021, com a maior concentração de publicações que discutiram as dificuldades de implementar e adaptar a LGPD ao contexto dos dispositivos IoT. Esse destaque pode estar relacionado ao período de adaptação da legislação brasileira de proteção de dados, como também ao aumento das discussões sobre sua aplicação em diferentes setores. Além disso, outros desafios como a segurança e a coleta de consentimento também aparecem ao longo dos anos, demonstrando preocupações persistentes, mas o gráfico permite visualizar mudanças de foco.

Gráfico 6 – Desafios explorados ao longo dos anos



Fonte: Autoria própria (2025)

5.8 Respostas às questões de pesquisa

Esta seção vai apresentar as respostas das questões de pesquisa estabelecidas, com base na análise dos estudos selecionados para o mapeamento sistemático. Cada subseção trata de uma questão específica, destacando as abordagens, contextos, desafios e contribuições encontradas. Portanto, o objetivo é fornecer uma visão estruturada e crítica sobre a conformidade de soluções em Internet das Coisas (IoT) com a Lei Geral de Proteção de Dados (LGPD).

5.6.1 **RQ1:** Quais são as abordagens propostas para garantir a conformidade com a LGPD em dispositivos IoT?

Os estudos analisados no mapeamento sistemático apresentam abordagens para garantir a conformidade dos dispositivos IoT de acordo com os princípios e exigências da Lei Geral de Proteção de Dados Pessoais (LGPD). Essas abordagens apontam soluções tecnológicas quanto estratégias jurídicas, normativas e organizacionais. A seguir, são destacadas as principais categorias identificadas.

As abordagens Jurídicas oferecem diversos estudos que apresentam interpretações legais e normativas da LGPD aplicadas aos dispositivos IoT, discutindo conceitos como consentimento, conceitos legais, finalidade e minimização de dados. Alguns trabalhos destacam a necessidade de ajustar os dispositivos e suas aplicações às obrigações legais existentes, como o uso de bases legais adequadas e a proteção de dados sensíveis, principalmente no contexto da saúde. A atuação dos agentes de tratamento, os direitos dos titulares e o papel da Autoridade Nacional de Proteção de Dados (ANPD) também são abordados de forma detalhada.

Vários estudos aplicaram a anonimização como estratégia para minimizar os riscos à privacidade. Essa técnica aparece principalmente em contextos sensíveis, como sistemas hospitalares e dispositivos vestíveis, buscando impedir a identificação de titulares de dados mesmo em casos de vazamentos. A adoção de *Privacy by Design (PbD)*, modos de privacidade e restrições automatizadas de compartilhamento são soluções técnicas recorrentes nesse grupo de estudos.

Outra abordagem envolvendo modelos e estruturas para avaliação da conformidade dos dispositivos e sistemas IoT com a LGPD. Os estudos verificam se o ciclo de vida do dado está em conformidade com os princípios da legislação. A ideia central é proporcionar a integração da proteção de dados desde a concepção do projeto, garantindo a documentação das decisões tomadas pelos agentes de tratamento. Alguns trabalhos propõem o uso de checklists como instrumentos práticos para guiar desenvolvedores e organizações na implementação de projetos com IoT. Esses checklists funcionam como ferramentas de verificação, organizadas com base nos princípios da LGPD, e são aplicáveis a diferentes domínios, como dispositivos vestíveis.

As abordagens exploram o uso de tecnologias como blockchain. A proposta é utilizar estruturas para garantir que os dados estejam sob controle dos titulares, com registros imutáveis de consentimento e rastreamento de acesso. Essa solução tecnológica é apresentada

como formas promissoras de alinhar as exigências legais com as capacidades dos sistemas IoT.

A Machine Learning é uma abordagem que faz o uso de aprendizado de máquina, como uma ferramenta de apoio à privacidade. Um estudo destaca um modelo capaz de identificar automaticamente dados pessoais sensíveis (PII) em grandes volumes de informações geradas por dispositivos IoT. Onde os algoritmos são treinados com dados anonimizados ou sob técnicas que evitam exposição indevida, e conformidade legal.

Alguns estudos também propõem modelos de governança, essa abordagem combina dimensões organizacionais, com definição de políticas internas, protocolos de segurança, capacitação de equipes e a criação de estruturas para a gestão contínua da privacidade. Em alguns casos, são utilizados para mapear riscos e implementar planos de resposta.

Ao agrupar essas abordagens, observa-se um esforço crescente em tratar a privacidade nos dispositivos IoT de forma integrada, considerando tanto os desafios técnicos quanto às exigências normativas e operacionais da LGPD.

Entre os destaques, a categoria jurídica foi a mais representada, indicando preocupação da literatura com a interpretação e aplicação da LGPD. Tecnologias emergentes como blockchain e machine learning também foram identificadas, ainda que com menor frequência, mas revelando grande potencial de contribuição para soluções.

Como direcionamento de pesquisa, nota-se a necessidade de estudos que aprofundem a aplicação prática dessas tecnologias emergentes, e a elaboração de mecanismos mais eficazes de consentimento e controle de dados. Além disso, investigações futuras podem explorar a integração entre abordagens jurídicas e técnicas, podendo promover soluções mais completas para a proteção de dados pessoais em ambientes conectados.

5.6.2 Q2: Em quais contextos os dispositivos IoT são aplicados nos estudos que abordam LGPD?

Os estudos analisados no mapeamento sistemático apontam que os dispositivos de IoT têm sido aplicados em vários contextos, destacando as áreas que envolvem dados sensíveis e interações com o usuário.

A área da saúde está presente em 9 dos 23 estudos analisados, com foco no monitoramento de pacientes, coleta de sinais vitais e gestão de dados sensíveis em ambientes clínicos. Cidades Inteligentes foram abordadas em 3 estudos, ligadas à gestão pública de dados, segurança urbana e serviços inteligentes. As aplicações em ambientes casas inteligentes (Smart Homes) e em Veículos Conectados foram menos frequentes, com 1 estudo

cada, o que demonstra um espaço ainda em crescimento para pesquisa futura.

O setor da Saúde foi um dos contextos mais mencionados nos estudos analisados. O uso de dispositivos como smartwatches, sensores médicos, marca-passos inteligentes, sistemas de monitoramento remoto e plataformas hospitalares foram explorados em soluções indicadas à coleta de sinais vitais, monitoramento de pacientes e apoio a diagnósticos. Esse contexto apresenta riscos enormes devido ao tratamento de dados sensíveis, como informações clínicas, que exigem conformidade com a LGPD. Diversos estudos destacam a necessidade de anonimização, segurança na transmissão de dados e governança da informação nos ambientes hospitalares e de pesquisa clínica.

Alguns estudos mostraram o uso de dispositivos IoT no ambiente doméstico, incluindo smart speakers, geladeiras inteligentes, sistemas de automação residencial e assistentes pessoais. Esses dispositivos realizam coleta contínua de dados pessoais e comportamentais, na maioria das vezes sem o conhecimento do usuário, o que desafia princípios da LGPD como transparência, necessidade e consentimento. As cidades inteligentes foram abordadas em 3 estudos, especialmente no uso de dispositivos conectados para gestão pública de dados, segurança urbana e serviços inteligentes.

Um estudo de caso abordou veículos conectados como sistemas IoT complexos, capazes de coletar dados de geolocalização, rotas, hábitos de direção, e até dados sensíveis, como o estado de saúde do condutor. A situação automotiva envolve desafios regulares e procura soluções específicas de governança da privacidade, alinhadas aos princípios da LGPD e a modelos de negócio da indústria automotiva. A utilização de tecnologias como Privacy by Design, Privacy-Enhancing Technologies e modos de privacidade foram apontadas como estratégias para reduzir os riscos de exposição de dados nesse domínio.

Em seguida, temos o grupo classificado como Geral, com 10 aplicações presentes nos estudos analisados. Esses estudos não se restringem a um domínio específico, mas discutem de forma abrangente os desafios de conformidade com a LGPD, aplicáveis a múltiplos contextos, como ambientes empresariais, residenciais e educacionais. Um dos artigos propõe o uso de checklists para avaliação de conformidade em diferentes tipos de dispositivos, reforçando a aplicabilidade das soluções de privacidade.

5.6.3 Q3: Quais desafios são apontados para a aplicação da LGPD em IoT?

Durante a análise dos 23 artigos selecionados no mapeamento sistemático, observou-se que, apesar dos diversos temas, alguns obstáculos se repetem com frequência significativa. Para melhor organização, esses desafios foram agrupados em quatro categorias

principais: Consentimento, que abrange as dificuldades na obtenção e gestão do consentimento informado dos titulares dos dados; Segurança e proteção de dados, relacionada às fragilidades técnicas e organizacionais na questão de preservação, confidencialidade e disponibilidade das informações; Regulamentações, que envolve lacunas na aplicação prática da LGPD e desafios de adaptação normativa; e Limitações técnicas, incluindo barreiras tecnológicas e estruturais que dificultam a implementação de soluções efetivas para garantir a privacidade.

A coleta silenciosa, e contínua de dados, dispositivos IoT realizam a coleta automatizada e constante de dados, muitas vezes sem interação explícita com o usuário. Essa característica dificulta o cumprimento de princípios da LGPD, como a transparência, a autodeterminação e o consentimento livre e informado. Usuários muitas vezes desconhecem que estão fornecendo dados e essa coleta silenciosa, associada à ausência de notificações claras, a falta do consentimento, mostram a fragilidade do modelo de consentimento na IoT, principalmente na ausência de informação, como na saúde pública, na automação doméstica ou em populações com baixo letramento digital. O usuário na maioria das vezes aceita termos sem pleno entendimento, o que contraria a LGPD sobre o consentimento válido e destacado.

Bases legais e uso indevido, a LGPD permite o tratamento de dados sem consentimento em algumas hipóteses, como para cumprimento de obrigação legal, execução de políticas públicas ou legítimo interesse do controlador. No entanto, os estudos analisados criticam o uso incomum e incorreto dessas bases legais, o que pode abrir brechas para abusos. Ainda mais na área da saúde, onde foi observada a insegurança jurídica quanto à definição do tratamento necessário e os limites da aplicação de bases como a proteção da vida ou interesse legítimo.

A ausência de técnicas e de segurança, a falta de padrões técnicos de segurança nos dispositivos IoT é citada como um dos principais obstáculos à conformidade com os princípios de segurança e prevenção previstos na LGPD. Muitos dispositivos operam de forma fraca, com ausência de criptografia, atualizações automáticas sem controle, e vulnerabilidades conhecidas, expondo dados sensíveis a riscos de interceptação ou vazamento.

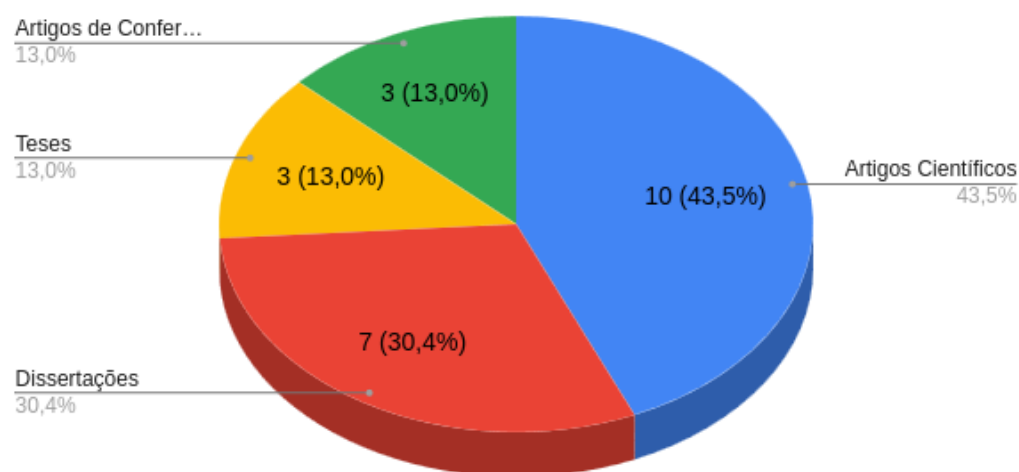
E a falta de regulamentação, por fim, os estudos mostram que a ausência de regulamentações específicas para IoT e a atuação ainda da Autoridade Nacional de Proteção de Dados (ANPD) dificultam a aplicação prática da LGPD. A LGPD estabelece princípios gerais, mas não define critérios técnicos claros para setores como a saúde, automotivo ou domicílios conectados, o que deixa falhas importantes na proteção de dados pessoais em

ambientes tecnológicos.

5.6.5 QA1: Quais são os tipos dos trabalhos científicos publicados?

No Gráfico 7, é identificada uma predominância em artigos científicos publicados em revistas científicas, com uma contagem de 10 dos 23 artigos analisados, isso demonstra que o tema vem sendo explorado com profundidade e rigor acadêmico. As dissertações de mestrado, contabilizam sete estudos e as teses de doutorado contabilizam três estudos que evidenciam o interesse de programas de pós-graduação em discutir a conformidade da LGPD no contexto da IoT, tanto em abordagens teóricas quanto aplicadas. Além disso, também foram identificados três artigos científicos apresentados em conferências, onde indicam que a discussão também está presente em fóruns técnicos e científicos mais dinâmicos, nos quais novas abordagens são testadas e compartilhadas com a comunidade.

Gráfico 7 - Tipos de trabalhos científicos



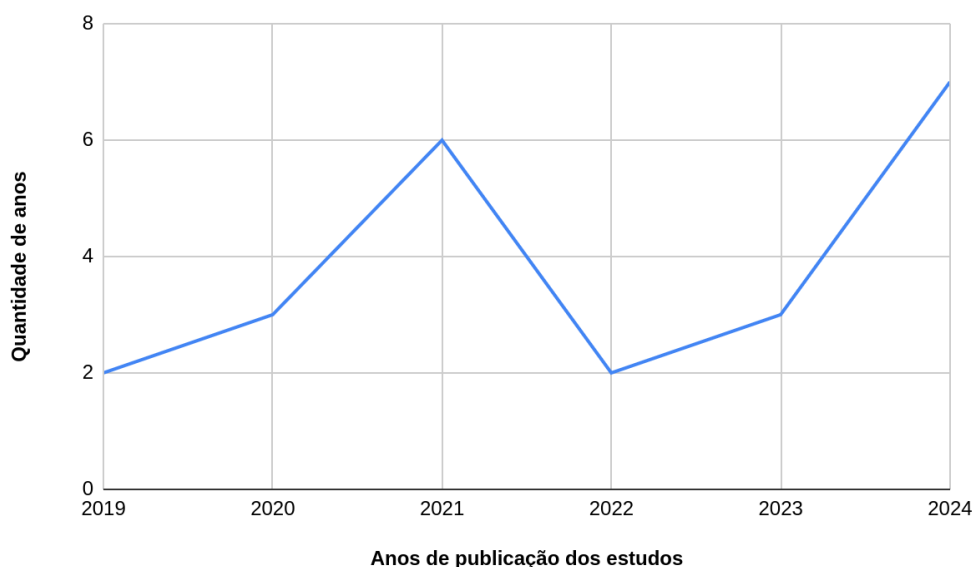
Fonte: Autoria própria (2025)

5.6.6 QA2: Como o número de publicações é distribuído ao longo dos anos?

No Gráfico 8 é possível identificar que a distribuição das 23 publicações analisadas possui um crescimento constante no interesse acadêmico sobre a conformidade da LGPD em dispositivos IoT ao longo dos anos. Em 2019, os primeiros dois estudos sinalizam a necessidade do tema no cenário brasileiro. A partir de 2020, observa-se uma elevação significativa nas publicações, atingindo um primeiro pico em 2021, com seis trabalhos. Em

2023, com três estudos, o volume também se manteve elevado, refletindo um contexto de amadurecimento regulatório e desenvolvimento de abordagens técnicas. O ano de 2024 aumentou o volume com cerca de sete trabalhos, evidenciando uma retomada do interesse, possivelmente associada à consolidação da LGPD e à ampliação do uso de tecnologias IoT em setores sensíveis como saúde, mobilidade e residências inteligentes.

Gráfico 8 - Anos de publicação dos estudos

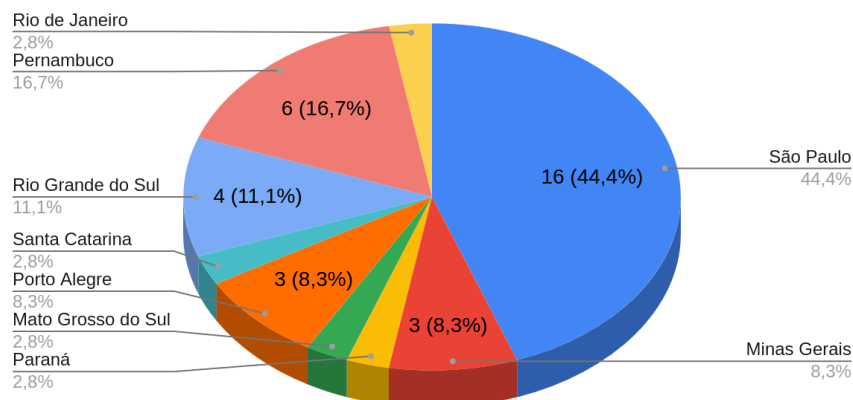


Fonte: Autoria própria (2025)

5.6.7 QA3: Quais são os locais de filiação dos autores?

Analisando o Gráfico 9 da afiliação dos autores dos estudos revela uma forte presença das instituições brasileiras, com destaque para os estados de São Paulo, Minas Gerais e Rio Grande do Sul, que concentram a maior parte das universidades participantes. São Paulo lidera com 16 autores de instituições, seguido de Pernambuco com 6 autores e Rio Grande do Sul, também com quatro. Outros estados com participação incluem Mato Grosso do Sul, Porto Alegre, Paraná, Santa Catarina e Rio de Janeiro.

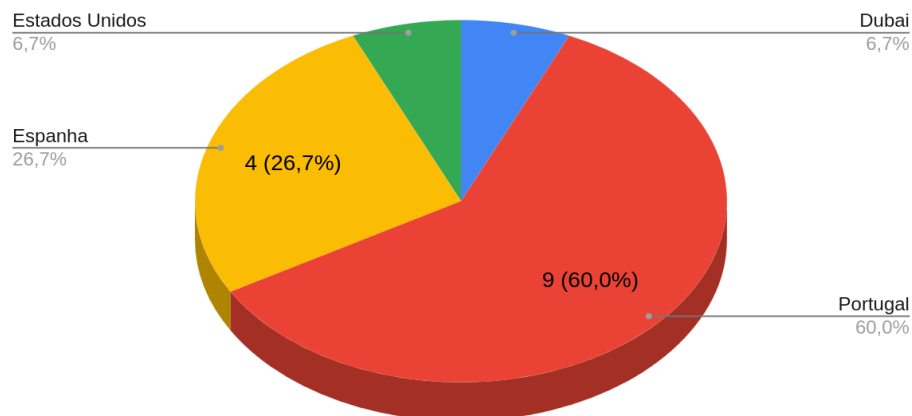
Gráfico 9 - Locais de afiliação dos autores nacionais



Fonte: Autoria própria (2025)

Também foram identificados autores de instituições internacionais. Estes podem ser observados no Gráfico 10, que mostra que foram identificadas contribuições de autores afiliados a instituições em Portugal com maior liderança, apresentando 9 autores por instituições, Espanha com apresenta um valor de 4 autores, Estados Unidos e Emirados Árabes. Essa diversidade geográfica evidencia que o debate sobre privacidade em dispositivos IoT e conformidade com a LGPD ultrapassa fronteiras nacionais, despertando interesse também em contextos acadêmicos estrangeiros, especialmente por semelhanças com outras legislações de proteção de dados.

Gráfico 10 - Locais de afiliação dos autores internacionais



Fonte: Autoria própria (2025)

5.9 Considerações finais dos resultados

Com a análise dos 23 estudos selecionados foi possível identificar uma diversidade de abordagens, contextos de aplicação, desafios e contribuições relacionadas à conformidade com a LGPD em dispositivos IoT. Dentre as abordagens, destacaram-se sete abordagens: Jurídico, Anonimização, Machine Learning, Avaliações de Conformidade, Checklist, Blockchain e Governança, sendo a abordagem Jurídico a mais recorrente entre os trabalhos.

Embora em menor número, abordagens que exploram *Machine Learning* e *Blockchain* têm ganhado interesse nos últimos anos, sendo consideradas tecnologias promissoras para a proteção de dados em ambientes conectados. O uso de Machine Learning aponta para soluções automatizadas na detecção de dados sensíveis e na aplicação dinâmica de regras de privacidade. Já o Blockchain tem sido explorado como alternativa para garantir transparência, rastreabilidade e descentralização no controle de dados pessoais. A presença ainda que pequena dessas abordagens nos estudos analisados indica uma possível tendência de pesquisa futura, com espaço para amadurecimento e maior aplicação prática no contexto da LGPD e da IoT.

Quanto aos contextos de aplicação, observou-se uma concentração significativa de estudos voltados para aplicações gerais, além de destaque para áreas específicas como cidades inteligentes, smart homes e veículos conectados. Entretanto, a área da saúde se destaca entre os estudos analisados, apresentando um número significativo de publicações. Esse destaque se justifica pelo fato da área tratar dos dados sensíveis envolvidos, como informações clínicas, biométricas e comportamentais, onde exige cuidados redobrados no tratamento, armazenamento e compartilhamento.

Essa perspectiva mostra o interesse crescente na aplicação da LGPD em ambientes diversos dos dispositivos IoT, principalmente em contextos sensíveis como o da saúde, onde a proteção de dados pessoais é crítica.

Por fim, quanto aos desafios enfrentados nos estudos analisados, destaca-se à regulamentação, ressaltando a complexidade e as dificuldades na aplicação efetiva da LGPD em ambientes IoT. Em seguida, o consentimento foi apontado como um desafio, refletindo as barreiras na obtenção e gestão do consentimento informado dos titulares. A segurança na proteção de dados também mostrou uma preocupação significativa, abordando aspectos como a prevenção contra ataques cibernéticos. Por último, as limitações técnicas, a dificuldade de integrar mecanismos de privacidade nos dispositivos, representam obstáculos relevantes para a conformidade e a aplicação prática das soluções propostas.

Os gráficos desenvolvidos ao longo do capítulo podem contribuir para reforçar a percepção de que já há pontos significativos de estudos práticos, técnicos e jurídicos que buscam responder aos desafios impostos pela LGPD no contexto da Internet das Coisas.

6 CONSIDERAÇÕES FINAIS

O objetivo central desta pesquisa foi mapear sistematicamente os estudos que propõem abordagens para garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) em dispositivos da Internet das Coisas (IoT), respondendo a questões relacionadas, aos contextos de aplicação, aos desafios enfrentados e às características das publicações. Para isso, foram definidos critérios de inclusão e exclusão, resultando na análise de 23 estudos primários publicados entre 2019 e 2024.

Os resultados mostraram que as abordagens mais recorrentes concentram-se em técnicas de anonimização, criptografia, gestão de consentimento e controle de acesso, frequentemente aplicadas em setores sensíveis como saúde, cidades inteligentes e ambientes domésticos. Entre os principais desafios, destacam-se as limitações técnicas para implementar medidas seguras de proteção em dispositivos com recursos restritos, como a dificuldade de obter e gerenciar consentimento de forma adequada em ecossistemas distribuídos.

Apesar de avanços identificados, constatou-se que ainda há lacunas significativas na integração entre princípios da LGPD e sistemas IoT, especialmente em soluções técnicas e requisitos jurídicos. A maioria das propostas permanece em estágio conceitual ou teórico, carecendo de validação prática em cenários reais.

Para ampliações futuras, oportunidades para o desenvolvimento de frameworks que possam combinar aspectos técnicos e jurídicos de forma aplicada, com validação em ambientes reais. Recomenda-se também ampliar o propósito do presente trabalho para setores pouco explorados, como agricultura, indústria 4.0 e educação, além de aprofundar a análise sobre impactos éticos e sociais do uso de dados pessoais em dispositivos inteligentes.

6.1 Trabalhos futuros

Para que possamos dar continuidade a este trabalho é interessante destacar algumas propostas para aprimoramento, como:

- **A aplicação de revisão sistemática:** Para que possa integrar e complementar com critérios ainda mais rigorosos e aprofundados para ampliar ainda mais os estudos identificados neste mapeamento.
- **Exploração de técnicas emergentes, como blockchain e machine learning:** Considerar essas tecnologias, que mesmo com poucos estudos presentes, ainda apresentam um grande potencial para a privacidade e a conformidade legal em dispositivos IoT.

- **Foco em cenários menos explorados:** Como ambientes industriais e educacionais, ampliando o alcance dos estudos para além dos contextos mais comuns.

REFERÊNCIAS

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: a Survey. **Computer Networks**, v. 54, n. 15, p. 2787–2805, 28 out. 2010.

BRASIL. LEI No 13.709, DE 14 DE AGOSTO DE 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

CARRION, Patrícia; QUARESMA, Manuela. Internet das Coisas (IoT): definições e aplicabilidade aos usuários finais. **HFD**, v. 8, n. 15, p. 49-66, mar. 2019. Disponível em: <http://dx.doi.org/10.59652316796308152019049>.

FALBO, R. d. A. Mapeamento Sistemático. 2018. Retrieved October, 2018.

FUKUDA, Leonardo Massami. Segurança da informação em IoT. Disponível em: https://repositorio.utfpr.edu.br/jspui/bitstream/1/19442/2/CT_GETIC_VIII_2019_05.pdf
Acesso em: 18 jul. 2025.

GODOI, Maiko Gustavo de; ARAÚJO, Liriane Soares. A INTERNET DAS COISAS: evolução, impactos e benefícios. **Revista Interface Tecnológica**, Taquaritinga, SP, v. 16, n. 1, p. 19–30, 2019. Disponível em: <https://revista.fatectq.edu.br/interfacetecnologica/article/view/538>. Acesso em: 19 jul. 2025.

MORAES, J. M. de; QUIRINO, C.; ALMEIDA, R. M. de .; NEVES, J. E. D. A. Internet das Coisas (IoT) : casa inteligente, definições e aplicações. **Revista Brasileira em Tecnologia da Informação**, [S. l.], v. 4, n. 2, p. 31 - 37, 2022. Disponível em: <https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/52>. Acesso em: 19 jul. 2025.

OLIVEIRA, N. S. DE 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, n. 4, 26 nov. 2019.

KITCHENHAM, B. A.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. Keele, 2007.

STALLINGS, W. Criptografia e segurança de redes. 6ª ed. São Paulo: Pearson, 2015.

PETERSEN, K. et al. Systematic Mapping Studies in Software Engineering. 1 jun. 2008.

WOHLIN, C., RUNESON, P., SILVEIRA NETO, P.A.M., ENGSTRÖM, E., MACHADO, I.C., ALMEIDA, E.A., On the Reliability of Mapping Studies in Software Engineering, **Journal of Systems and Software**, vol. 86, n. 10, 2013, pp 2594 - 2610.

WOHLIN, C., RUNESON, P., HÖST, M., OHLSSON, M.C., REGNELL, B., WESSLÉN, A., Experimentation in Software Engineering, Springer, 2012.

GONÇALVES DE OLIVEIRA, J. et al. **XIX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO -ENANCIB 2018 GT-8 -Informação e Tecnologia INTERNET DAS COISAS E PRIVACIDADE: UMA REVISÃO SISTEMÁTICA DA LITERATURA THE INTERNET OF THINGS AND PRIVACY: A SYSTEMATIC REVIEW OF LITERATURE** Modalidade da Apresentação: Comunicação Oral. [s.l.:

s.n.]. Disponível em:

<https://repositorio.ufmg.br/bitstream/1843/51456/2/INTERNET%20DAS%20COISAS%20E%20PRIVACIDADE%20UMA%20REVIS%3%83O%20SISTEM%3%81TICA%20DA%20LITERATURA.pdf> Acesso em: 3 jun. 2025.

ARANTES, Guilherme Jannotti. Observabilidade em sistemas de Internet das Coisas: um mapeamento sistemático. 2021. 38 f. Monografia (Graduação em Sistemas de Informação) - Instituto de Ciências Exatas e Aplicadas, Universidade Federal de Ouro Preto, João Monlevade, 2021. Disponível em: <https://www.monografias.ufop.br/handle/35400000/3304>. Acesso em: 03 jun. 2025.

COSTA, R. B. A lei geral de proteção de dados pessoais aplicada à internet das coisas: uma revisão sistemática, 2022. 72 f. Monografia (Graduação em Engenharia da Computação) - Campus de Sobral, Universidade Federal do Ceará, Sobral, 2022.

BERNARDI, E. et al. Brazilian scenarios for smart cities deployment from public policies perspectives. **2022 IEEE International Smart Cities Conference (ISC2)**, p. 1–8, 28 set. 2020.

NADELLA, D. Securing Data at Rest: Using ML-Driven Personally Identifiable Information(PII) Detection and Privacy-Preserving Techniques. **2024 International Conference on Engineering and Emerging Technologies (ICEET)**, p. 1–5, 27 dez. 2024.

JORGE EDUARDO RIVADENEIRA et al. A Blockchain-Based Privacy-Preserving Model for Consent and Transparency in Human-Centered Internet of Things. 9 maio 2023.

CALAZA, T. Evolução e regulação da privacidade e proteção de dados no contexto da internet das coisas no cenário brasileiro. **Revista do CAAP**, v. 29, n. 1, p. 1–18, 9 set. 2024.

BIANCHI, D.; CONSALTER, G. proteção da privacidade pela lei geral de proteção de dados (lgpd) na era da internet das coisas (iot). **Revista de Direito**, v. 16, n. 02, p. 01-30, 14 nov. 2024.

COLETI, T. A. et al. Handling of Personal Data by Smart Home Equipment: an Exploratory Analysis in the Context of LGPD. **Journal on Interactive Systems**, v. 15, n. 1, p. 311–322, 30 mar. 2024.

BIN, K. J. et al. Digital Platform for Continuous Monitoring of Patients Using a Smartwatch: Longitudinal Prospective Cohort Study. **JMIR Formative Research**, v. 7, p. e47388–e47388, 2 ago. 2023.

LIMBERGER, T.; DA, G.; GIANNAKOS, S. Internet das coisas (IoT) e os direitos à privacidade e à proteção de dados do cidadão: uma necessária aproximação. **Revista Brasileira de Políticas Públicas**, v. 13, n. 3, 16 fev. 2024.

VERRI LUCCA, A. et al. A Case Study on the Development of a Data Privacy Management Solution Based on Patient Information. **Sensors (Basel, Switzerland)**, v. 20, n. 21, p. E6030, 23 out. 2020.

DAL MAGRO, D.; FORTES, V. B. O reconhecimento facial nas smart cities e a garantia dos direitos à privacidade e à proteção de dados pessoais. **Revista de Direito Internacional**, v. 18, n. 2, 12 nov. 2021.

FORNASIER, M. D. O. The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy. **Revista de Investigações Constitucionais**, v. 6, n. 2, p. 297, 29 nov. 2019.

CARVALHO DA SILVA, NIVALDO. **GOVERNANÇA E PRIVACIDADE DE DADOS PESSOAIS: estudo de caso dos usuários de veículos conectados na perspectiva da indústria à luz da Lei Geral de Proteção de Dados Brasileira (LGPD)**. 2021. 206 f. Dissertação (Mestrado) - PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS, [S. l.], 2021.

GOMES NETO, Ivonildo Pereira. Estendendo um checklist de inspeção da aderência de soluções à LGPD para avaliar critérios específicos de IoT. 2022. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2022.

ZEFERINO, André Ferreira. A privacidade está on? Uma avaliação nos textos de políticas de privacidade e termos de uso de Artefatos IoT em relação à lei geral de proteção de dados. 2021. 63 f. Dissertação (Mestrado em Humanidades Digitais) - Instituto Multidisciplinar de Nova Iguaçu, Universidade Federal Rural do Rio de Janeiro, Nova Iguaçu, 2021.

ALBANDES, Rogério da Costa. Abordagem IoT PD-RPM: Promovendo Aderência à Diálise Peritoneal Considerando o Cenário da Internet das Coisas. Orientador: Adenauer Corrêa Yamin. 2024. 144 f. Tese (Doutorado em Ciência da Computação) – Centro de Desenvolvimento Tecnológico, Universidade Federal de Pelotas, Pelotas, 2024.

CASTRO, BÁRBARA BRITO DE. **Direito Digital na Era da Internet Das Coisas – O Direito à Privacidade e o Sancionamento da Lei Geral de Proteção de Dados Pessoais**. Disponível em:

<https://ambitojuridico.com.br/direito-digital-na-era-da-internet-das-coisas-o-direito-a-privacidade-e-o-sancionamento-da-lei-geral-de-protecao-de-dados-pessoais/>

EDUARDO, C. Coleta, utilização indevida e proteção de dados no ambiente digital na legislação brasileira: a internet das coisas como sistema de transferência de dados pessoais. **Uninove.br**, 2024.

RUVIARO, Eduardo Missau. **(Des) proteção de dados e internet das coisas: os desafios à tutela dos dados de saúde de usuários de dispositivos de IOT à luz dos preceitos da LGPD**. 2021. Dissertação (Mestrado) - Universidade Federal de Santa Maria, [S. l.], 2021.

RONCATTO, Carolina da Rosa. **Internet das coisas e responsabilidade civil: os riscos do desenvolvimento dos dispositivos**. 2022. Dissertação (Mestrado) - Universidade Federal do Rio Grande do Sul, [S. l.], 2022.

BIN, Kaio Jia. **Modelo de captura de dados por internet das coisas e disponibilização dos mesmos para uso clínico e de pesquisa seguindo as leis de proteção de dados**. 2023. Tese (Doutorado em Educação e Saúde) - Faculdade de Medicina, Universidade de São Paulo, São Paulo, 2023. doi:10.11606/T.5.2023.tde-06022024-135139. Acesso em: 2025-07-27.

Camara, Maria Amália Arruda, et al. “Internet Das Coisas E Blockchain No Sistema Único de Saúde: A Proteção Dos Dados Sensíveis Diante Da Lei Geral de Proteção de Dados.”

Cadernos Ibero-Americanos de Direito Sanitário, vol. 10, no. 1, 18 Mar. 2021, pp. 93–112, <https://doi.org/10.17566/ciads.v10i1.657>.

SILVEIRA, S. A. Segurança da informação e proteção de dados pessoais: estudo de caso e proposta de governança para serviços de saúde. 2021. 211 p. Dissertação (Mestrado Profissional em Inovação Tecnológica) - Instituto de Ciência e Tecnologia - Universidade Federal de São Paulo - UNIFESP, São José dos Campos, 2021.

LANNES, Yuri Nathan da Costa. Nova privacidade no Brasil e os impactos jurídicos e econômicos: uma análise do big data e da responsabilidade empresarial. 2020. 125 f. Tese (Direito Político e Econômico) - Universidade Presbiteriana Mackenzie, São Paulo .