

## **ESTUDO BIBLIOMÉTRICO SOBRE A PROTEÇÃO DE DADOS NO CONTEXTO DA SEGURANÇA CIBERNÉTICA EM CIDADES INTELIGENTES**

**ANDRE LOZANO FERREIRA**

UNIVERSIDADE PRESBITERIANA MACKENZIE (MACKENZIE)

**TATIANA DE SOUZA MENDES GARCIA**

UNIVERSIDADE PRESBITERIANA MACKENZIE (MACKENZIE)

Agradecimento à orgão de fomento:

O trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal - Brasil (CAPES 2024).

# ESTUDO BIBLIOMÉTRICO SOBRE A PROTEÇÃO DE DADOS NO CONTEXTO DA SEGURANÇA CIBERNÉTICA EM CIDADES INTELIGENTES

## 1 INTRODUÇÃO

No contexto da transformação digital e com o aumento de uso de tecnologias inovadoras em cidades inteligentes, surgem as vulnerabilidades e riscos de proteção de dados e segurança cibernética. Assim, o uso de tecnologias inovadoras, como sensores, dispositivos conectados e sistemas de gerenciamento integrados, oferece uma oportunidade para melhorar os serviços públicos, indiretamente o planejamento urbano e oferecer qualidade de vida aos cidadãos. No entanto, a transformação digital traz consigo desafios importantes de segurança cibernética que precisam ser estudados para garantir a proteção dos dados e de toda a infraestrutura urbana (Araújo, 2023).

A revolução informacional e tecnológica acelerada levantou muitas questões relativas à proteção de dados. A tecnologia avançou muito e o processamento e a coleta seguiram o curso, tornaram-se mais comuns em todas as áreas da vida, mais avançadas e certamente mais complexas. Assim, por meio dos dispositivos inteligentes, da Internet das Coisas (IoT), etc., um enorme volume de dados é trocado não só no setor privado, mas também no setor público. A vida cotidiana das pessoas foi amplamente reformulada devido à rápida disseminação da tecnologia digital, que também se estendeu ao funcionamento das cidades. As cidades inteligentes estão associadas a uma grande produção de dados. Consequentemente, as atividades e transações cotidianas dos cidadãos que utilizam *smartphones*, identificações digitais, cartões de crédito, cartões de viagem pessoais, etc., levantam preocupações relativamente ao respeito e à proteção da privacidade. A utilização de todos estes dados produzidos e a sua partilha é um verdadeiro desafio que requer abordagens inovadoras (Stefanouli & Economou, 2019).

Para Al-Huthaifi et al. (2023) as cidades inteligentes cresceram em popularidade, motivadas pelo número crescente de pessoas que vivem nas cidades, o que aumentou a pressão sobre o ambiente, as infraestruturas e os recursos. O número de cidades inteligentes aumentou muito com a mudança de cidades para cidades inteligentes e o estabelecimento de cidades inteligentes inteiramente novas. A China, por exemplo, está desenvolvendo mais de 200 iniciativas de novas cidades inteligentes (Lin, 2018). As cidades inteligentes diferem das cidades tradicionais em vários aspectos, incluindo elevada heterogeneidade dos utilizadores, elevado envolvimento dos utilizadores, restrições de recursos da IoT individual, elevada mobilidade de produtos e tecnologias, maior ligação dos utilizadores e escalabilidade do desenvolvimento. A implantação de tecnologias de informação e comunicação (TIC) e IoT em cidade inteligente aumenta o monitoramento e a integração de diversos sistemas de infraestrutura, resultando em decisões operacionais mais otimizadas. Como resultado, cidades inteligentes tornam as nossas cidades mais eficientes, habitáveis e sustentáveis. Os cidadãos de cidades inteligentes desfrutam de habitação inteligente, transporte inteligente, cuidados de saúde inteligentes e governança inteligente (Cui et al., 2018). O *big data* criado em cidades inteligentes, por outro lado, é vulnerável a ataques e hackers, criando dificuldades substanciais para a proteção da privacidade e sua segurança (Al-Huthaifi et al., 2023).

A literatura atual sobre proteção de dados em cidades inteligentes carece de um impulso mais pragmático, o que poderia tornar-se de grande importância tanto para aumentar a sensibilização do público como para influenciar diretamente os decisores políticos, especialmente à escala local. Isto pode ser conseguido combinando aspectos éticos e teóricos com soluções e cenários práticos. Portanto, o aprimoramento de estudos de proteção de dados

em cidades inteligentes, tanto de forma prática quanto filosófica, pode fornecer sugestões construtivas e importantes para a sociedade (Fabrègue & Bogoni, 2023).

Embora não se identifique na literatura um estudo abrangente de proteção de dados em cidades inteligentes, há uma clara necessidade de um estudo amplo que apoie a adoção de práticas de proteção de dados em todo o mundo (Vandercruysse et al., 2020). Assim, surge a seguinte questão: **Qual é a evolução da produção científica relacionada com a proteção de dados no contexto da segurança cibernética em cidades inteligentes?**

O objetivo geral é verificar a evolução da produção científica relacionada com a proteção de dados no contexto da segurança cibernética em cidades inteligentes. Quanto aos objetivos específicos foram propostas três investigações importantes: a) Identificar os principais estudos relacionados a práticas para a proteção de dados em cidades inteligentes; b) identificar os principais autores e clusters relacionados quando à produção científica de apoio à legislação de proteção de dados em cidades inteligentes e c) analisar a coocorrência de palavras-chave dos estudos relacionados à produção científica de proteção de dados e cidades inteligentes.

Segundo Bruzzeguez et al. (2024), cidades inteligentes trabalham com a coleta massiva de dados em tempo real sobre as mais diversas esferas de um ambiente urbano, e isso inclui, certamente, dados pessoais de cidadãos. Há, portanto, uma preocupação de governos e sociedade quanto às questões que envolvem a proteção de dados pessoais e a privacidade. As principais preocupações relacionadas à proteção e privacidade de dados pessoais e possível medidas de mitigação são: a) Vigilância e controle, b) uso comercial dos dados, c) vazamento de dados, d) usos não esperados (usos secundários), e) compartilhamento de dados de maneira inadequada, f) discriminação e aspectos éticos e g) perda da qualidade do dado. Assim, governos e comunidades devem priorizar a segurança cibernética na implementação de tecnologias nas cidades, exigindo altos padrões de segurança nas especificações técnicas em aquisições, utilizando-se de criptografia nos dados que trafegam no ecossistema da cidade inteligente, implementando monitoramento e controles de acesso na rede, conduzindo avaliações regulares de riscos de segurança da informação, dentre outros (Bruzzeguez et al., 2024).

Assim, estudos sobre proteção de dados no contexto da segurança cibernética em cidades inteligentes ainda são insuficientes. Embora existam pesquisas iniciais sobre o tema, faltam dados sobre os impactos após alguns anos de implementação e em decorrência do dinamismo da evolução do tema. Diante da relevância do tema, um estudo bibliométrico sobre a proteção de dados em cidades inteligentes pode apresentar contribuições para estudiosos, interessados pelo tema e especialistas, com a possibilidade de identificar lacunas importantes e até mesmo a necessidade de aprofundar estudos já realizados, com contribuições adicionais no contexto da segurança cibernética.

## **2 REFERENCIAL TEÓRICO**

Apresenta-se neste capítulo autores e pesquisas que dão suporte teórico para a pesquisa, em termos de proteção de dados e cidades inteligentes.

### **2.1 Proteção de Dados**

A proteção de dados refere-se às ações adotadas para garantir a segurança, a integridade e a confidencialidade das informações pessoais e sensíveis das pessoas ou organizações. O objetivo da proteção de dados é prevenir o acesso não autorizado, uso indevido, divulgação ou perda de dados, garantindo que as informações sejam tratadas de

forma ética e em conformidade com as leis e regulamentos de privacidade. Os princípios da proteção de dados incluem a) confidencialidade, b) integridade, c) disponibilidade, d) consentimento, e) minimização da coleta de dados, f) segurança e g) transparência. A proteção de dados é essencial para garantir a privacidade e a segurança das informações pessoais em um mundo cada vez mais digital. Organizações e governos devem adotar práticas de proteção de dados mais robustas para proteger a privacidade dos indivíduos e manter a confiança em relação ao tratamento das informações pessoais (Fabrègue & Bogoni, 2023).

Para Fabrègue e Bogoni (2023) a importância da privacidade de dados e da proteção da informação na construção de uma comunidade urbana inteligente de sucesso é fundamental para fortalecer a confiança dos cidadãos. Os residentes precisam sentir que seus dados estão seguros e que sua privacidade está sendo respeitada para apoiar plenamente o desenvolvimento urbano inteligente. Neste sentido, o respeito aos direitos individuais e a prevenção de abusos e discriminação fazem parte do mesmo pacote. A prevenção dos ataques cibernéticos são o maior ganho diante de ações de proteção de dados e privacidade.

Vandercruysse et al. (2020) referem-se à proteção de dados como as práticas e medidas adotadas para garantir a segurança, privacidade e integridade das informações pessoais de indivíduos ou organizações. Isso envolve o controle e a gestão adequada dos dados pessoais para garantir que sejam usados de maneira ética, legal e segura.

As leis de proteção de dados são essenciais para a salvaguarda dos dados e estabelecem diretrizes e requisitos específicos para a coleta, armazenamento, processamento e compartilhamento de dados pessoais. Essas regulamentações visam proteger os direitos e a privacidade dos indivíduos, garantindo que seus dados sejam tratados de forma transparente e segura. A proteção de dados é fundamental em um mundo cada vez mais digital, onde a quantidade de informações pessoais coletadas e utilizadas é significativa. Garantir a proteção adequada dos dados não apenas fortalece a confiança dos usuários, mas também ajuda a prevenir violações de privacidade, fraudes e uso indevido das informações pessoais (Vandercruysse et al., 2020).

Entretanto, para Fabrègue e Bogoni (2023) as soluções propostas para proteger a privacidade e segurança da informação em cidades inteligentes têm sido consideradas insuficientes por diferentes razões, considerando as limitações na coleta de dados, protocolos de comunicação defeituosos e vulnerabilidades em dispositivos e sistemas. Devido à dificuldade de acesso direto aos dados, os pesquisadores foram obrigados a buscar proxies, como relatórios e leis, o que pode levar a uma compreensão limitada do assunto. Falhas nos protocolos de comunicação podem resultar em preocupações com a privacidade, mesmo na ausência de problemas de segurança. Protocolos defeituosos podem vaziar informações além da finalidade pretendida, comprometendo a privacidade dos dados de forma desnecessária. Dispositivos inteligentes, como IoT, dispositivos vestíveis e sistemas autônomos, podem conter vulnerabilidades de segurança que permitem invasões na privacidade dos usuários. Sendo assim, fundamental a necessidade de revisão ética e legal.

Assim, garantir a proteção adequada dos dados não apenas fortalece a confiança dos usuários, mas também ajuda a prevenir violações de privacidade, fraudes e uso indevido das informações pessoais. Em resumo, a privacidade de dados e a proteção da informação desempenham um papel crucial na construção de uma comunidade urbana inteligente de sucesso, promovendo a confiança dos cidadãos, respeitando os direitos individuais, prevenindo abusos e discriminação, garantindo a segurança cibernética e assegurando a conformidade legal e ética. Portanto, é essencial priorizar a privacidade e a segurança da informação em iniciativas de cidades inteligentes para garantir um ambiente urbano sustentável e inclusivo (Fabrègue & Bogoni, 2023; Vandercruysse et al., 2020).

## 2.2 Cidades Inteligentes

A cidade inteligente como campo de pesquisa desenvolveu-se rapidamente desde o final da década de 1990, quando o conceito foi introduzido pela primeira vez (Anthopoulos, 2015). A adoção do termo cidade inteligente gerou dúvidas quanto ao seu significado, pois há divergências na literatura científica sobre quando ou como uma cidade se torna inteligente (Vandercruysse et al., 2020). Em primeiro lugar, uma vertente da literatura centra-se principalmente nos aspectos puramente tecnológicos subjacentes ao desenvolvimento e aos processos urbanos (Talari et al., 2017), ou seja, a cidade inteligente representa a capacidade tecnológica urbana em seu auge. Em segundo lugar, inteligente é utilizado para significar o nível de educação da população urbana, ou seja, pessoas inteligentes que se reúnem em áreas urbanas, resultando em cidades que se tornam inteligentes (Crutzen & Kummitha, 2017).

As cidades inteligentes diferem das cidades tradicionais em diferentes aspectos, incluindo heterogeneidade e envolvimento dos utilizadores, uso de recursos da IoT, mobilidade de produtos e tecnologias, ligação dos utilizadores e escalabilidade do desenvolvimento. A implantação de TIC e IoT em cidades inteligentes aumenta o monitoramento e a integração de diversos sistemas, resultando em decisões operacionais mais otimizadas. Como resultado, cidades inteligentes tornam as cidades mais eficientes, habitáveis e sustentáveis. O *big data* criado em cidades inteligentes, por outro lado, é vulnerável a ataques e hackers, criando dificuldades substanciais para a privacidade e a segurança (Al-Huthaifi et al., 2023).

Uma cidade inteligente é uma cidade que utiliza TIC e dados para melhorar a qualidade de vida dos cidadãos, a eficiência operacional dos serviços urbanos e a sustentabilidade ambiental. O objetivo da cidade inteligente é criar ambientes urbanos mais conectados, sustentáveis, seguros e inclusivos. Além disso, as cidades inteligentes promovem a participação cidadã, a transparência governamental e a inovação colaborativa para enfrentar desafios urbanos complexos. Ao adotar abordagens inovadoras e centradas no cidadão, as cidades inteligentes buscam melhorar a qualidade de vida, promover o desenvolvimento econômico e reduzir o impacto ambiental, tornando-se mais resilientes e preparadas para o futuro (Vandercruysse et al., 2020).

Da mesma forma, para Fabrègue e Bogoni (2023), uma cidade inteligente é uma área urbana que utiliza TIC para melhorar a qualidade de vida dos cidadãos, promover a sustentabilidade ambiental, otimizar a infraestrutura urbana e serviços públicos, e impulsionar o desenvolvimento econômico. Em uma cidade inteligente, diversos dispositivos e sensores são integrados à infraestrutura urbana para coletar dados em tempo real, permitindo uma gestão mais eficiente e eficaz dos recursos. Esses dados são então analisados para fornecer insights e informações que podem ser utilizados para tomar decisões informadas e melhorar a experiência dos residentes.

Alguns dos principais elementos de uma cidade inteligente incluem: a) Conectividade: Infraestrutura de rede robusta que permite a comunicação entre dispositivos e sistemas em toda a cidade; b) Coleta de dados: Sensores e dispositivos IoT que coletam informações sobre diversos aspectos urbanos, como tráfego, qualidade do ar, consumo de energia, entre outros; c) Análise de dados: Utilização de análise de dados e inteligência artificial para interpretar as informações coletadas e gerar insights acionáveis; d) Serviços inteligentes: Implementação de serviços públicos inteligentes, como transporte público eficiente, iluminação pública automatizada, gestão de resíduos inteligente, entre outros; e) Participação cidadã: Promoção da participação ativa dos cidadãos no planejamento e na gestão da cidade, por meio de plataformas digitais e aplicativos móveis. Assim, uma cidade

inteligente busca integrar tecnologia, inovação e sustentabilidade para criar um ambiente urbano mais eficiente, seguro, inclusivo e sustentável para seus habitantes (Fabrègue & Bogoni, 2023).

Em resumo, uma cidade inteligente é uma cidade que utiliza TIC (Fabrègue & Bogoni, 2023; Talari et al., 2017; Vandercruysse et al., 2020), por meio de sensores IoT (Al-Huthaifi et al., 2023; Fabrègue & Bogoni, 2023) e dados (Al-Huthaifi et al., 2023) para melhorar a qualidade de vida dos cidadãos (Al-Huthaifi et al., 2023; Fabrègue & Bogoni, 2023; Vandercruysse et al., 2020), a eficiência operacional dos serviços urbanos (Al-Huthaifi et al., 2023; Fabrègue & Bogoni, 2023; Vandercruysse et al., 2020) e a sustentabilidade ambiental (Al-Huthaifi et al., 2023; Fabrègue & Bogoni, 2023; Vandercruysse et al., 2020), criando um big data (Al-Huthaifi et al., 2023; Fabrègue & Bogoni, 2023), apoiando no desenvolvimento econômico (Vandercruysse et al., 2020) e na inovação constante de serviços (Fabrègue & Bogoni, 2023) na busca de maior eficiência IoT (Al-Huthaifi et al., 2023; Fabrègue & Bogoni, 2023).

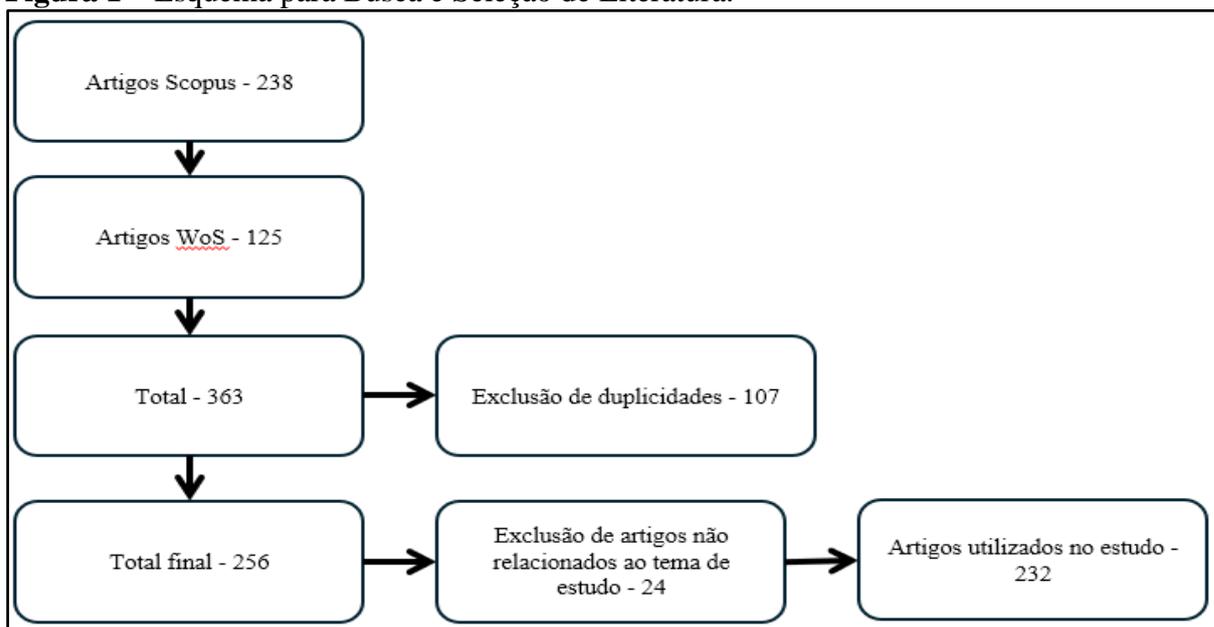
### 3 PROCEDIMENTOS METODOLÓGICOS

Um estudo bibliométrico foi realizado para o propósito deste estudo. A bibliometria, assim como outros tipos de estudos bibliométricos, requer cuidados específicos por parte dos pesquisadores, dentre os quais, destacam-se a relevância e o rigor. Chueke e Amatucci (2015) afirmam que o rigor implica decisões relacionadas ao design da pesquisa e o atendimento às premissas do método escolhido, contemplando as principais leis da bibliometria (Bradford, Zipf, Lotka), que regem esses estudos (Silva, 2022).

A Lei de Lotka (1926) ou Lei do Quadrado Inverso propõe que um número restrito de pesquisadores produz muito em determinada área de conhecimento, enquanto um grande volume de pesquisadores produz pouco. A Lei de Bradford (Bogaert et al., 2000) possibilita estimar o grau de relevância de periódicos que atuam em áreas do conhecimento específicas, assim, periódicos com maior publicação de artigos sobre determinado assunto tendem a estabelecer um núcleo supostamente de qualidade superior e maior relevância nesta área do conhecimento. A Lei de Zipf ou Lei do Mínimo Esforço (Guedes & Borschiver, 2005) consiste em medir a frequência do aparecimento das palavras em vários textos, gerando uma lista ordenada de termos de uma determinada disciplina ou assunto (Machado Junior et al., 2016).

A pesquisa utilizou a técnica de data mining posicionando-se assim como um estudo quantitativo que segundo Richardson et al. (1985), caracteriza-se pela quantificação da coleta de informações, e pelo emprego de técnicas no tratamento dos dados, de forma independente à sua complexidade (Machado Junior et al., 2016). Várias etapas compõem o data mining, que por sua vez se inicia na seleção das bases de dados sobre as quais será realizado o processamento. O esquema que mostra as diferentes etapas relacionadas a seleção das bases de dados é apresentado na Figura 1. Para o estudo foram selecionadas as bases de dados *Scopus* e *Web of Science (WoS)*. As bases de dados foram consultadas e a extração dos dados foi realizada no mês de junho de 2024. Os termos de pesquisa utilizados foram “*data protection*” e “*smart cit\**”. O item “*\**” foi utilizado nos comandos de pesquisa para que outras variantes da palavra *city* pudessem ser incluídas, como *cities*, por exemplo.

**Figura 1** – Esquema para Busca e Seleção de Literatura.



Fonte: Elaborado pelos autores.

Na base de dados *Web of Science (WoS)* utilizou-se o termo de pesquisa: TS = ("*data protection*") AND TS = ("*smart cit\**"). Ao todo, foram identificados 125 documentos. Na base de dados Scopus foi utilizado o termo de pesquisa: (TITLE-ABS-KEY ("*data protection\**") AND TITLE-ABS-KEY ("*smart cit\**")) e foram encontrados 238 documentos. O total de documentos identificados foi de 363, sendo que 104 documentos da base de dados Scopus foram excluídos por constarem em duplicidade. Para realizar a unificação da base de dados e a eliminação das duplicidades foi utilizado o programa RStudio®. Além disto três documentos foram identificados como duplicidade e excluídos manualmente, considerando análise realizada pelo número do DOI dos documentos. Restaram 256 documentos que foram analisados inicialmente pelo título e posteriormente pelo resumo, restando 232 documentos para compor o estudo bibliométrico. Não foram utilizados critérios de datas para restrição do período analisado.

Com a conclusão das definições da base de dados, se iniciou a aplicação de um processamento dos dados. Neste estudo, o processamento e a análise dos dados se desenvolveram por meio da elaboração de gráficos e dados, utilizando-se das ferramentas Bibliometrix® e VOSViewer®. O pós-processamento do *data mining* consiste na apresentação e análise dos dados da pesquisa, demonstrados a seguir.

#### 4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Segundo o estudo de Donthu et al. (2021), para atingir os objetivos específicos deve-se utilizar um ou mais relatórios específicos, como indicado na Figura 2.

**Figura 2** - Relação Objetivo Específico e Relatório de Análise.

Objetivos específicos	Relatório de Análise / Descrição	Referência de apoio
a) Identificar os principais estudos relacionados a práticas para a proteção de dados em cidades inteligentes.	Análise de citações - Analisar as relações entre as publicações, identificando as publicações mais influentes em um campo de pesquisa.	Podsakoff et al. (2005)
b) identificar os principais autores e clusters relacionados	Análise de coautoria - Examinar o Interações sociais ou relações entre	Acedo et al. (2006)

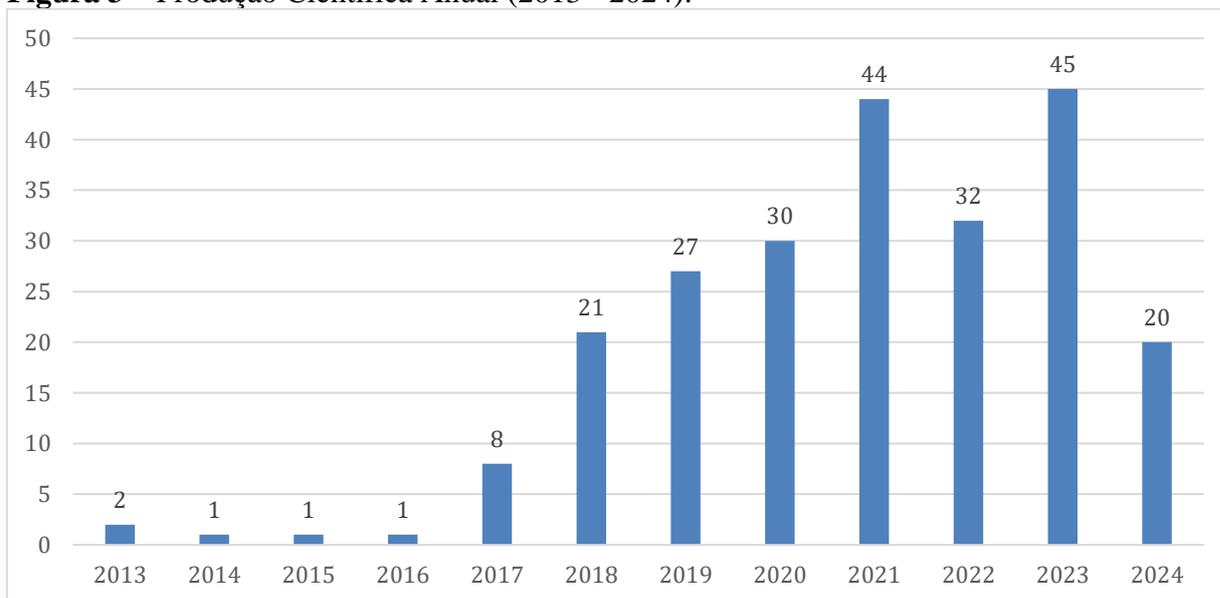
Objetivos específicos	Relatório de Análise / Descrição	Referência de apoio
quando à produção científica de apoio à legislação de proteção de dados em cidades inteligentes.	autores e suas afiliações e equivalentes impactos no desenvolvimento da pesquisa campo.	
c) analisar a coocorrência de palavras-chave dos estudos relacionados à produção científica de proteção de dados e cidades inteligentes.	Análise de coocorrência - Explorar as relações existentes ou futuras entre tópicos de um campo de pesquisa, concentrando-se no conteúdo escrito da própria publicação.	Emich et al. (2020)

Fonte: Elaborado pelos autores, com base em Donthu et al. (2021).

Para cada um dos objetivos específicos apresentados na Figura 2, foram criados relatórios específicos para o seu atingimento, entretanto relatórios complementares foram agregados ao estudo no intuito de aprofundar as análises e o entendimento aprofundado da abordagem utilizada.

As análises iniciais apresentam dados relevantes para a pesquisa, considerando que foram identificados estudos no período de 2013 a 2024, 160 periódicos, 232 documentos no total, com crescimento anual de 23,28%, o que representa um tema em ascensão. Os documentos apresentam em média 10,92 citações e utilizam 663 referências.

**Figura 3** – Produção Científica Anual (2013 - 2024).



Fonte: Elaborado pelos autores, com base nos dados gerados pelo Bibliometrix®.

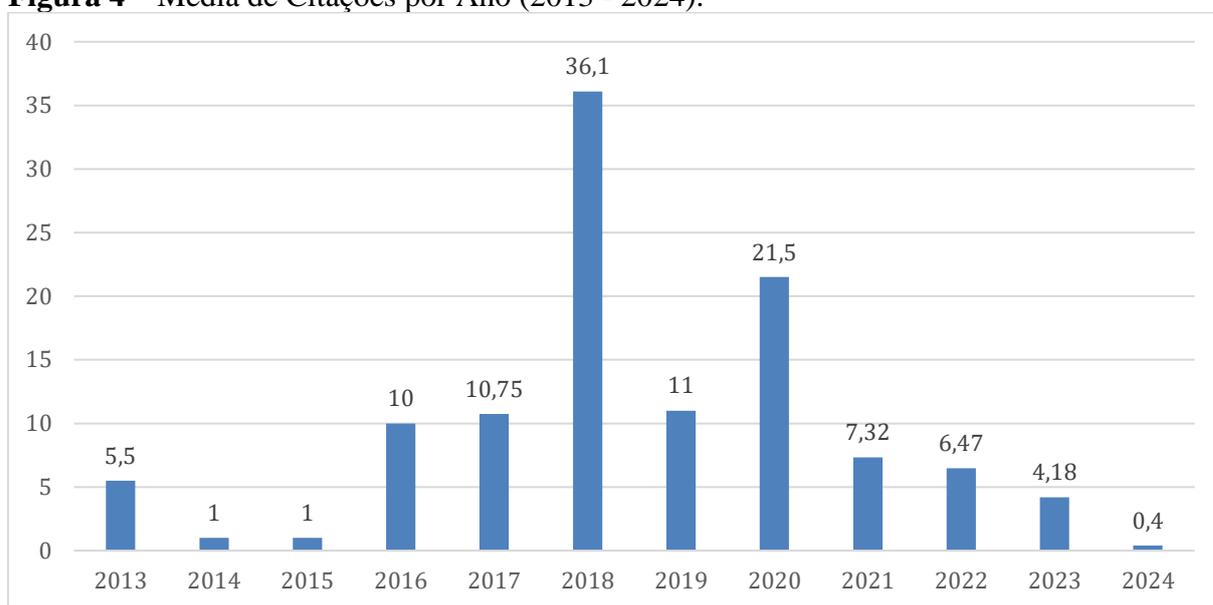
A Figura 3 apresenta a evolução anual da produção científica do tema proteção de dados e cidades inteligentes para o período de 2013 a 2024. O ano de 2024 possui os dados parciais, considerando a data da pesquisa, mas apresenta informações relevantes para o estudo, assim foram mantidas na Figura 3.

A análise de citações é uma técnica fundamental para o mapeamento científico. Ela parte do pressuposto de que as citações refletem conexões intelectuais entre publicações, formadas quando uma obra menciona outra. Nesse contexto, o impacto de uma publicação é determinado pelo número de vezes que ela é citada. Essa análise permite identificar as obras mais influentes em um determinado campo de pesquisa. Embora existam diversos métodos, como métricas de rede, para avaliar a importância das publicações em uma área de

investigação, a citação direta permanece a medida mais objetiva e direta do impacto. Portanto, por meio das citações, como demonstrado na Figura 4, é possível compreender a dinâmica intelectual desse campo (Donthu et al., 2021).

Para Podsakoff et al. (2005), a análise profunda das citações permite identificar a influência dos periódicos no campo de estudo, considerando a média de citações por artigo, bem como identificar as tendências significativas na influência destes periódicos. A Figura 4 apresenta a evolução da média de citações por ano no período de 2013 a 2024, sendo que o ano de 2018 apresentou o maior número médio de citações, representando 36,1 de valor médio, representando um aumento significativo em relação à média total de 10,52 citações. O ano de 2018 representa o início de maior produção científica e deve ser considerado nas análises de citação como um período importante para o tema de proteção de dados e cidades inteligentes.

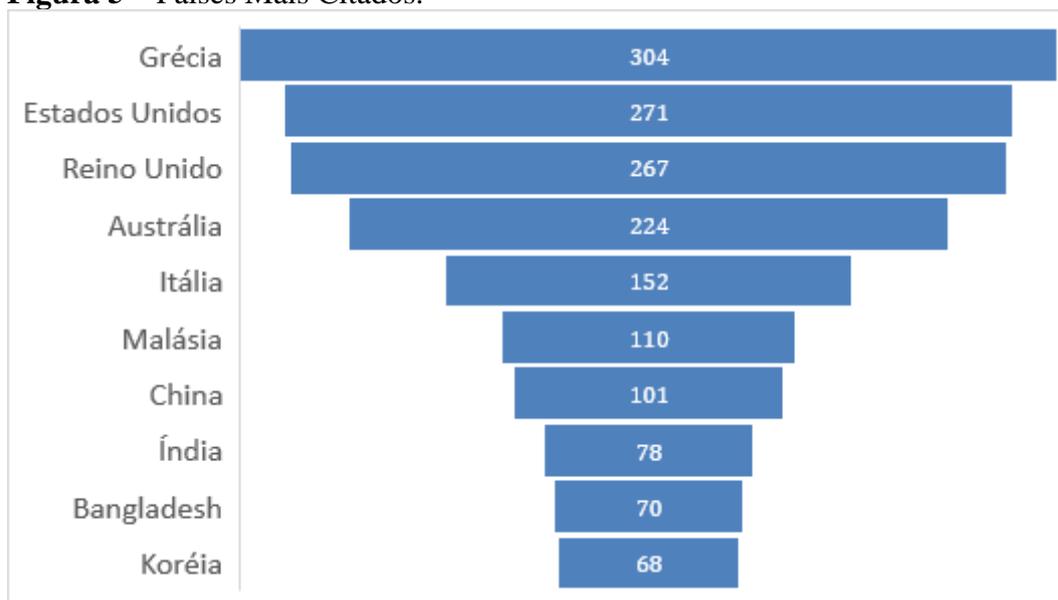
**Figura 4** – Média de Citações por Ano (2013 - 2024).



Fonte: Elaborado pelos autores, com base nos dados gerados pelo Bibliometrix®.

Uma das análises relevantes é identificar os países mais citados. Neste estudo, foi identificado que a Grécia tem 304 citações, ocupando destaque em relação a países como Estados Unidos com 271 citações e o Reino Unido, com 267 citações, como demonstra a Figura 5. Vale destacar que a Figura 5 apresenta os 10 países mais citados no mundo.

**Figura 5 – Países Mais Citados.**



Fonte: Elaborado pelos autores, com base nos dados gerados pelo Bibliometrix®.

Os documentos mais citados globalmente são apresentados na Tabela 1, gerado com o apoio do Bibliometrix®. Destaca-se, por exemplo, o artigo *Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research* (Lytras & Visvizi, 2018) que analisa o debate sobre cidades inteligentes na perspectiva de, por um lado, a sensibilização dos cidadãos para aplicações e soluções que são consideradas “inteligentes” e, por outro lado, a sua capacidade de utilizar aplicações e soluções.

**Tabela 1 – Documentos Mais Citados Globalmente.**

Documentos	Total de citações
Lytras, M. D., & Visvizi, A. (2018). Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research. <i>Sustainability</i> , 10(6), 1998.	290
Liang, F., Yu, W., An, D., Yang, Q., Fu, X., & Zhao, W. (2018). A survey on big data market: Pricing, trading and protection. <i>Ieee Access</i> , 6, 15132-15154.	230
Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. <i>Computers &amp; Security</i> , 88, 101653.	207
Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. <i>IEEE Access</i> , 8, 23601-23623.	101
Nandy, T., Idris, M. Y. I. B., Noor, R. M., Kiah, L. M., Lun, L. S., Juma'at, N. B. A., ... & Bhattacharyya, S. (2019). Review on security of internet of things authentication mechanism. <i>IEEE Access</i> , 7, 151054-151089.	96
Calzada, I. (2018). (Smart) citizens from data providers to decision-makers? The case study of Barcelona. <i>Sustainability</i> , 10(9), 3252.	90
Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuahya, M. A., Bairagi, A. K., Khan, M. A. M., & Kee, S. H. (2022, October). IoT-based healthcare-monitoring system towards improving quality of life: A review. In <i>Healthcare</i> (Vol. 10, No. 10, p. 1993). MDPI.	70
Sonn, J. W., & Lee, J. K. (2020). The smart city as time-space cartographer in COVID-19 control: the South Korean strategy and democratic control of surveillance technology. <i>Eurasian Geography and Economics</i> , 61(4-5), 482-492.	68
Streitz, N., Charitos, D., Kaptein, M., & Böhlen, M. (2019). Grand challenges for ambient	57

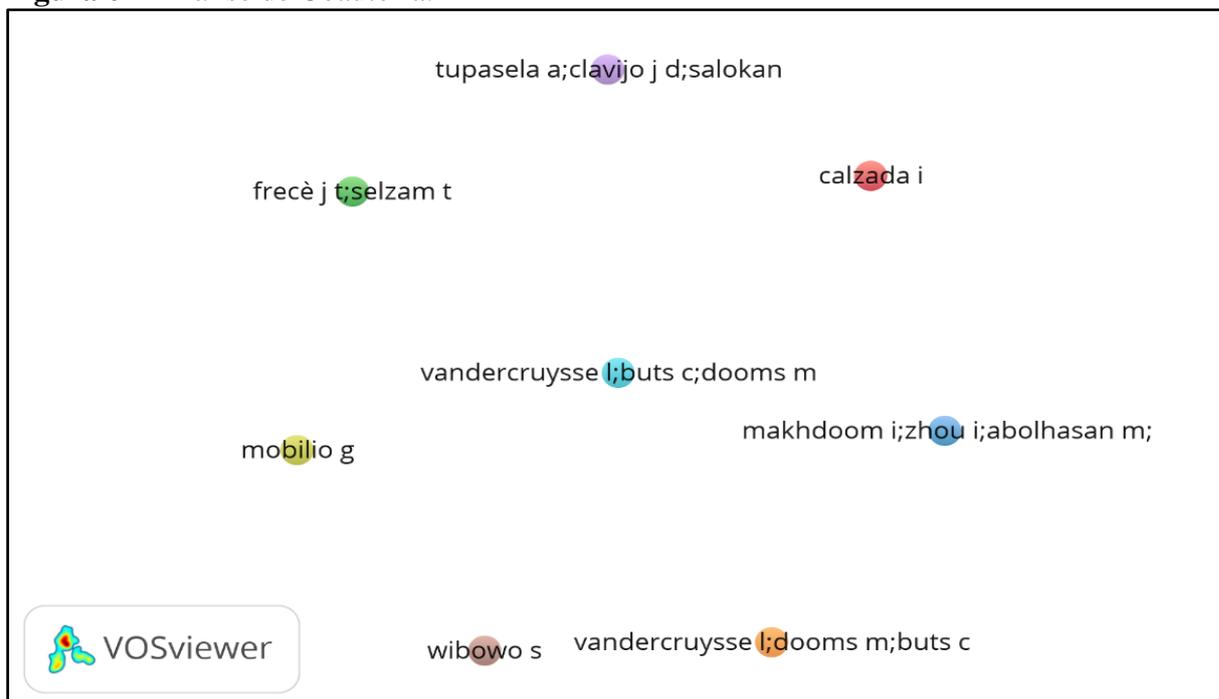
Documentos	Total de citações
intelligence and implications for design contexts and smart societies. Journal of Ambient Intelligence and Smart Environments, 11(1), 87-107.	
Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR compliant blockchains—a systematic literature review. Ieee Access, 9, 50593-50606.	52

Fonte: Elaborado pelos autores, com base nos dados gerados pelo Bibliometrix®.

A análise de coautoria tem o objetivo de examinar as interações sociais ou relações entre autores e suas afiliações e equivalentes impactos no desenvolvimento da pesquisa campo de pesquisa. Com a crescente complexidade metodológica e teórica na pesquisa, as colaborações entre acadêmicos tornaram-se um lugar comum. A análise também permite que as colaborações sejam mapeadas em diferentes períodos de tempo, permitindo assim que os acadêmicos revisem a trajetória do desenvolvimento intelectual em relação às redes de colaboração, ao mesmo tempo que equipam os futuros acadêmicos com informações valiosas para alcançar e colaborar com acadêmicos estabelecidos e em tendência na pesquisa (Acedo et al., 2006).

Conforme constata-se na Figura 6, foram identificados oito clusters considerando os dados gerados pelo VOSViewer®. Os clusters apresentados demonstram a importância do autor Vandercruysse et al. (2020) para o tema, bem como diferentes autores e seus relacionamentos. Considerando o volume de dados encontrados e o curto período de análise de 2013 a 2024, sendo 2024 um valor parcial, não foram identificados períodos que justificassem o corte ou mapeamento em diferentes períodos para comparação.

**Figura 6** – Análise de Coautoria.



Fonte: Dados de pesquisa, elaborado com VOSViewer®.

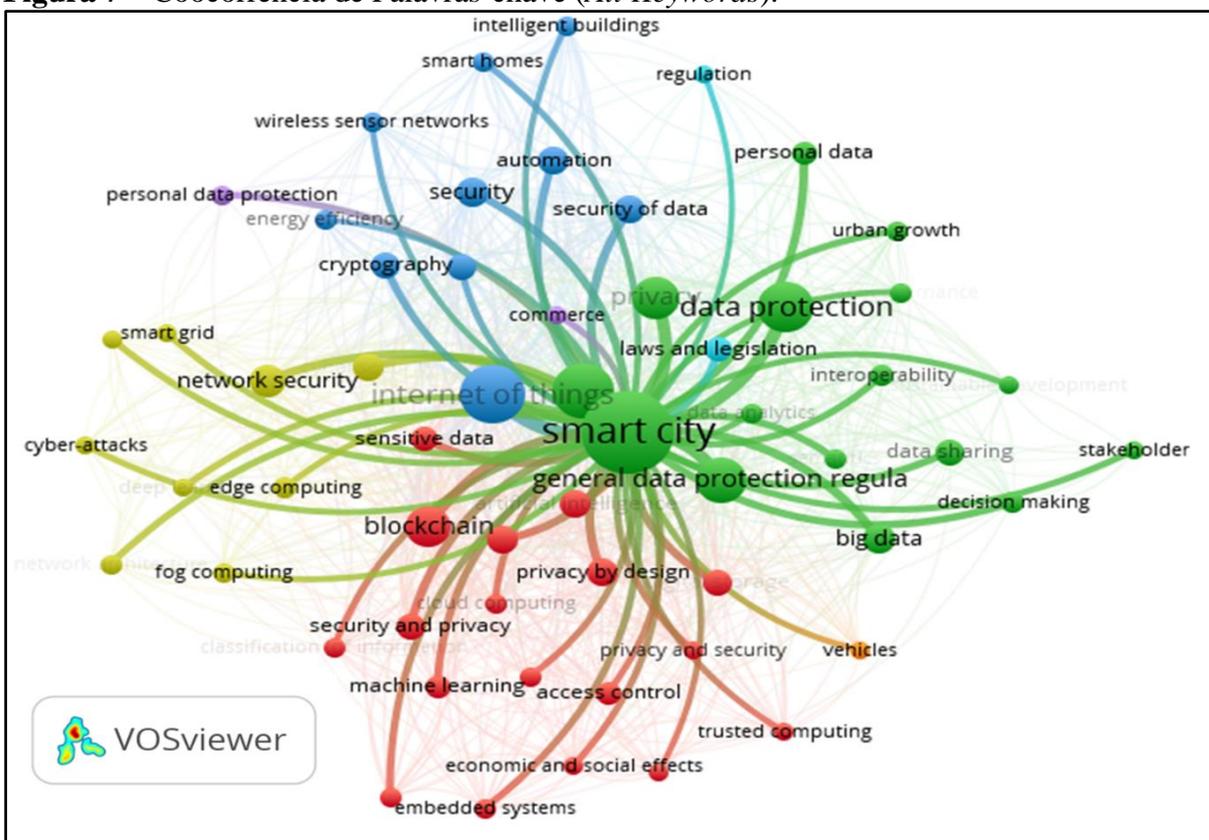
Complementarmente, a análise de coocorrência de palavras-chave tem por objetivo explorar as relações existentes ou futuras entre tópicos de um campo de pesquisa, concentrando-se no conteúdo escrito da própria publicação (Donthu et al., 2021). No estudo, foram identificadas 58 palavras-chave que aparecem pelo menos 5 vezes entre 2013 e 2024. Assim, foram calculadas as frequências de termos de uma palavra, por exemplo, liderança, e

termos de duas palavras, por exemplo, eficácia coletiva, presentes nos títulos e resumos dos artigos desse período. Os resultados indicaram que as palavras-chave capturaram os principais tópicos do *corpus* ao longo de sua vida e que os termos mais recentes foram geralmente adicionados às principais áreas temáticas, e não removidos delas.

Então, foram analisadas as palavras-chave no período de 2013 a 2024, sem exclusão de nenhum termo. Foi usado o software VOSviewer® para visualizar as diversas interações de rede para a análise de mapeamento (Van Eck & Waltman, 2012). Para detectar clusters, o VOSviewer® começa criando uma matriz de similaridade baseada na coocorrência de palavras-chave em cada artigo. As medidas de coocorrência são usadas para calcular a força da associação entre os nós.

A força da associação é usada como entrada para a função de modularidade de Newman e Girvan (2004), onde a modularidade para cada nó é calculada com base em sua associação com outros nós do *cluster*. Cada nó é colocado em um *cluster* no qual sua modularidade é máxima. O processo continua até que todos os nós atinjam sua maior modularidade.

**Figura 7** – Coocorrência de Palavras-chave (*All Keywords*).



Fonte: Dados de pesquisa, elaborado com VOSViewer®.

O VOSviewer® utiliza dois pesos padronizados: centralidade de grau, ou seja, o número total de laços relacionais que um nó possui, e força total do link, ou seja, o número total de links multiplicado pelo peso de cada link (Van Eck & Waltman, 2012). Foi utilizado o VOSviewer® para criar visualizações de redes baseadas em gráficos. O tamanho do nó, como demonstrado na Figura 7, representa a importância de um nó dentro da rede, enquanto as arestas conectadas representam a força de um relacionamento, neste caso, o número de artigos que tiveram a coocorrência das palavras-chave vinculadas. Desta forma, tanto a colocação dos nós como a força dos laços indicam conectividade conceptual. Os nós pertencentes à mesma comunidade são da mesma cor.

Assim, foram identificados no processamento do VOSViewer® 58 itens, 7 clusters, 793 links, com força total de 2177. No *cluster 1 (blockchain)* foram identificados 18 itens, no *cluster 2 (smart city)*, 16 itens, no *cluster 3 (internet of things)*, 10 itens, no *cluster 4 (network security)*, 9 itens, no *cluster 5 (personal data protection)*, 2 itens, no *cluster 6 (laws and legislation)*, 2 itens e no *cluster 7 (vehicle)*, 1 item.

## 5 CONSIDERAÇÕES FINAIS

O objetivo deste estudo foi verificar a evolução da produção científica relacionada com as ações de proteção de dados no contexto da segurança cibernética em cidades inteligentes. No contexto da transformação digital e o aumento do uso de tecnologias inovadoras em cidades inteligentes, surgem as vulnerabilidades e riscos de privacidade de dados e segurança cibernética. Neste contexto, embora não se identifique na literatura um estudo abrangente de proteção de dados em cidades inteligentes, há uma clara necessidade de um estudo amplo que apoie a adoção de legislação de proteção de dados em todo o mundo.

As análises iniciais apresentam dados relevantes para a pesquisa, considerando que foram identificados estudos no período de 2013 a 2024. Ao todo, foram localizados um total de 160 periódicos e 232 documentos, com crescimento anual de 23,28%, o que indica um tema em ascensão. Os documentos apresentam em média 10,92 citações cada, e utilizam 663 referências.

Os principais resultados apontam que estudos da Grécia são os mais citados, seguido de Estados Unidos e Reino Unido. Dentre os documentos mais citados, destaca-se, por exemplo, o artigo *Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research* (Lytras & Visvizi, 2018) que analisa o debate sobre cidades inteligentes na perspectiva de, por um lado, a sensibilização dos cidadãos para aplicações e soluções que são consideradas “inteligentes” e, por outro lado, a sua capacidade de utilizar aplicações e soluções. Os clusters apresentados na análise de coautoria demonstram a importância do autor Vandercruysse et al. (2020) para o tema, bem como diferentes autores e seus relacionamentos. Na análise de coocorrência de palavras-chave, identifica-se a importância de clusters relacionados a temas de proteção e segurança, como *blockchain* e *general data protection*.

O estudo bibliométrico apresenta resultados importantes, como a identificação do estado da arte da literatura. Diante das questões relacionadas ao conceito de cidades inteligentes, recomenda-se estudos futuros com maior profundidade para temas específicos, como a proteção de dados em temas de *big data* para cidades inteligentes, a eficiência operacional dos serviços urbanos e inovação, inclusive em cidades brasileiras, considerando contextos e momento de transição ou transformação digital das grandes cidades. Vale destacar que o tema inteligência artificial surgiu em uma quantidade reduzida de estudos. Diante do cenário de evolução tecnológica, conexões 5G e serviços digitais nas cidades inteligentes, recomenda-se avaliar o impacto do uso da inteligência artificial para a proteção de dados no contexto da segurança cibernética em cidades inteligentes.

As limitações para este estudo estão relacionadas ao período de sua execução. Considerando o dinamismo que o tema apresenta, recomenda-se a definição de modelos de proteção de dados em cidades inteligentes que possam ser analisados em relação à frameworks duradouros e flexíveis, baseados na colaboração entre entidades governamentais, públicas e privadas.

O estudo identifica resultados importantes e lacunas que direcionam para o aprofundamento de estudos futuros para ampliar a contribuição à sociedade em temas de

proteção de dados em cidades inteligentes e contribui com interessados, estudiosos e especialistas que buscam a inovação e a agilidade nas soluções de problemas relacionados.

## REFERÊNCIAS

- Acedo, F. J., Barroso, C., Casanueva, C., & Galán, J. L. (2006). Co-Authorship in Management and Organizational Studies: An Empirical and Network Analysis\*. *Journal of Management Studies*, 43(5), 957–983. <https://doi.org/10.1111/j.1467-6486.2006.00625.x>
- Al-Huthaifi, R., Li, T., Huang, W., Gu, J., & Li, C. (2023). Federated learning in smart cities: Privacy and security survey. *Information Sciences*, 632, 833–857. <https://doi.org/10.1016/j.ins.2023.03.033>
- Anthopoulos, L. G. (2015). Understanding the Smart City Domain: A Literature Review. Em M. P. Rodríguez-Bolívar (Org.), *Transforming City Governments for Successful Smart Cities* (Vol. 8, p. 9–21). Springer International Publishing. [https://doi.org/10.1007/978-3-319-03167-5\\_2](https://doi.org/10.1007/978-3-319-03167-5_2)
- Araújo, G. (2023). *Segurança cibernética em cidades inteligentes para proteção dos Dados e da infraestrutura urbana*. Inforchannel. <https://inforchannel.com.br/2023/09/06/seguranca-cibernetica-em-cidades-inteligentes-para-protecao-dos-dados-e-da-infraestrutura-urbana/>
- Bogaert, J., Rousseau, R., & Van Hecke, P. (2000). Percolation as a model for informetric distributions: Fragment size distribution characterised by Bradford curves. *Scientometrics*, 47(2), 195–206. <https://doi.org/10.1023/A:1005678707987>
- Bruzzeguez, G. A., Moraes, T. G., & Guedes, M. S. (2024). *Cidades Inteligentes*. Autoridade Nacional de Proteção de Dados. [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao\\_radar\\_tecnologico\\_jan\\_2024.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf)
- Chueke, G. V., & Amatucci, M. (2015). O que é bibliometria? Uma introdução ao Fórum. *Internext*, 10(2), 1–5. <https://doi.org/10.18568/1980-4865.1021-5>
- Crutzen, D. N., & Kummitha, D. R. (2017). *How do we understand Smart City? An Evolutionary Perspective*. <https://doi.org/10.1016/j.cities.2017.04.010>
- Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access*, 6, 46134–46145. <https://doi.org/10.1109/ACCESS.2018.2853985>
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, 133, 285–296. <https://doi.org/10.1016/j.jbusres.2021.04.070>
- Emich, K. J., Kumar, S., Lu, L., Norder, K., & Pandey, N. (2020). Mapping 50 Years of Small Group Research Through *Small Group Research*. *Small Group Research*, 51(6), 659–699. <https://doi.org/10.1177/1046496420934541>
- Fabrègue, B. F. G., & Bogoni, A. (2023). Privacy and Security Concerns in the Smart City. *Smart Cities*, 6(1), 586–613. <https://doi.org/10.3390/smartcities6010027>
- Guedes, V. L., & Borschiver, S. (2005). Bibliometria: Uma ferramenta estatística para a gestão da informação e do conhecimento, em sistemas de informação, de comunicação e de avaliação científica e tecnológica. *Encontro nacional de ciência da informação*, 6(1), 18.

- Lin, Y. (2018). A comparison of selected Western and Chinese smart governance: The application of ICT in governmental management, participation and collaboration. *Telecommunications Policy*, 42(10), 800–809. <https://doi.org/10.1016/j.telpol.2018.07.003>
- Lotka, A. J. (1926). The frequency distribution of scientific productivity. *Journal of the Washington Academy of Sciences*, 16(12), 317–323.
- Lytras, M., & Visvizi, A. (2018). Who Uses Smart City Services and What to Make of It: Toward Interdisciplinary Smart Cities Research. *Sustainability*, 10(6), 1998. <https://doi.org/10.3390/su10061998>
- Machado Junior, C., Souza, M. T. S. D., Parisotto, I. R. D. S., & Palmisano, A. (2016). As Leis da Bibliometria em Diferentes Bases de Dados Científicos. *Revista de Ciências da Administração*, 111–123. <https://doi.org/10.5007/2175-8077.2016v18n44p111>
- Newman, M. E. J., & Girvan, M. (2004). Finding and evaluating community structure in networks. *Physical Review E*, 69(2), 026113. <https://doi.org/10.1103/PhysRevE.69.026113>
- Podsakoff, P. M., MacKenzie, S. B., Bachrach, D. G., & Podsakoff, N. P. (2005). The influence of management journals in the 1980s and 1990s. *Strategic Management Journal*, 26(5), 473–488. <https://doi.org/10.1002/smj.454>
- Richardson, R. J., Peres, J. A., & Wanderley, J. C. V. (1985). *Pesquisa social: Métodos e técnicas*. Atlas.
- Silva, C. L. da. (2022). *Manual prático para estudos bibliométricos com o uso do Biblioshiny*. Ediupf.
- Stefanouli, M., & Economou, C. (Orgs.). (2019). *Data Protection in Smart Cities: Application of the EU GDPR* (Vol. 879). Springer International Publishing. [https://doi.org/10.1007/978-3-030-02305-8\\_90](https://doi.org/10.1007/978-3-030-02305-8_90)
- Talari, S., Shafie-khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. (2017). A Review of Smart Cities Based on the Internet of Things Concept. *Energies*, 10(4), 421. <https://doi.org/10.3390/en10040421>
- Van Eck, N. J., & Waltman, L. (2012). *VOSviewer Manual*. [https://www.vosviewer.com/documentation/Manual\\_VOSviewer\\_1.5.2.pdf](https://www.vosviewer.com/documentation/Manual_VOSviewer_1.5.2.pdf)
- Vandercruysse, L., Buts, C., & Dooms, M. (2020). A typology of Smart City services: The case of Data Protection Impact Assessment. *Cities*, 104, 102731. <https://doi.org/10.1016/j.cities.2020.102731>