



II CIGELUBRA

Congresso Internacional de Gestão e Engenharia Luso-Brasileiro

03 a 05 de dezembro de 2025

As Engenharias na Transformação Digital das PMEs

Cidades Inteligentes Seguras: o Papel das Tecnologias de Privacidade

Cristina Akemi Shimoda Uechi

Departamento de Engenharia de Produção – Universidade Tecnológica Federal do Paraná

Micaela de Araujo Freitas

TIC Timor

Regina Pagani

Departamento de Engenharia de Produção – Universidade Tecnológica Federal do Paraná

Hugo Valadares Siqueira

Departamento de Engenharia de Produção – Universidade Tecnológica Federal do Paraná

Resumo: Este artigo examina o papel das Tecnologias de Aprimoramento da Privacidade - PETs como soluções para os desafios de privacidade e proteção de dados em cidades inteligentes. Essas cidades utilizam tecnologias como internet das coisas, inteligência artificial, big data e 5G para inovar e melhorar a qualidade de vida, mas dependem da coleta massiva de dados pessoais, o que traz riscos de vigilância, uso indevido, ciberataques e vieses algorítmicos. A pesquisa, de abordagem exploratória e qualitativa, combinou revisão de literatura científica com análise de literatura cinzenta de órgãos nacionais e internacionais, utilizando o Methodi Ordinatio para seleção dos estudos. Os resultados apontam um ecossistema tecnológico diversificado para proteção de dados, destacando técnicas como anonimização, pseudonimização, criptografia, minimização de dados, computação de borda, dados sintéticos, processamento federado e blockchain. A inteligência artificial é usada tanto na coleta quanto na proteção e processamento seguro dos dados, e a computação quântica surge como tendência futura. O estudo também apresenta um panorama comparativo entre Brasil, Timor-Leste e China, evidenciando diferentes níveis de desenvolvimento urbano e regulamentação. Enquanto a China lidera em inovação e patentes, o Brasil destaca-se pela implementação da LGPD e políticas públicas, e Timor-Leste inicia sua infraestrutura digital. A pesquisa conclui que a adoção das PETs, junto a marcos legais sólidos, governança transparente, participação cidadã e cooperação internacional, é crucial para garantir a privacidade e promover cidades inteligentes mais seguras, éticas e centradas nas pessoas.

Palavras-chave: cidades inteligentes, proteção de dados, tecnologias de aprimoramento da privacidade.

Secure Smart Cities: The Role of Privacy-Enhancing Technologies

Abstract: This article explores the role of Privacy-Enhancing Technologies (PETs) as solutions to privacy and data protection challenges in smart cities. These cities leverage technologies such as the Internet of Things, artificial intelligence, big data, and 5G to drive innovation and improve quality of life, but they rely heavily on massive personal data collection, which raises risks of surveillance, misuse, cyberattacks, and algorithmic bias. This exploratory qualitative study combined a review of scientific literature with an analysis of grey literature from national and international organizations, employing the Methodi Ordinatio for study selection. The findings reveal a diverse technological ecosystem for data protection, highlighting techniques as anonymization, pseudonymization, encryption, data minimization, edge computing, synthetic data, federated learning, and blockchain. Artificial intelligence is applied not only in data collection but also in safeguarding and securely processing data, while quantum computing emerges as a promising future trend. The study also

provides a comparative overview of Brazil, Timor-Leste, and China, illustrating varying levels of urban development and regulatory frameworks. China leads in innovation and patents, Brazil advances with the implementation of the LGPD and public policies, and Timor-Leste is in the early stages of building its digital infrastructure. The research concludes that adopting PETs, alongside robust legal frameworks, transparent governance, citizen participation, and international cooperation, is essential to ensure privacy and foster smarter, safer, ethical, and human-centered cities.

Keywords: smart cities; data protection; privacy-enhancing technologies.

1. Introdução

O conceito de Cidades Inteligentes emergiu como uma resposta inovadora aos desafios urbanos contemporâneos, buscando aprimorar a qualidade de vida dos cidadãos, a eficiência dos serviços, a sustentabilidade e a resiliência dos espaços urbanos. A base desses projetos reside na utilização intensiva de Tecnologias da Informação e Comunicação - TICs, que permitem a coleta massiva de dados com grande precisão, qualidade e variedade. Tecnologias como Internet das Coisas - IoT, Big Data e Inteligência Artificial - IA são consideradas tecnologias essenciais para o funcionamento dessas cidades, impulsionando a automatização de serviços e o desenvolvimento de novas formas de interação e gestão urbana (FIGUEIREDO, 2022).

Contudo, essa proliferação tecnológica e a coleta massiva de dados pessoais e sensíveis dos cidadãos nas cidades inteligentes suscitam preocupações significativas em relação à privacidade e à proteção de dados (SOARES et al., 2023). A possibilidade de vigilância e controle, o uso comercial indevido de dados por fornecedores, que podem, por exemplo, capitalizar ao oferecer serviços gratuitos aos municípios, o desvio de finalidade por meio de usos secundários não esperados e o compartilhamento inadequado de informações entre setores público e privado são riscos eminentes. Incidentes como ciberataques, vazamentos de dados e a falta de priorização da segurança e privacidade no desenvolvimento e uso das tecnologias representam ameaças consideráveis (BRASIL, 2024b).

Diante desses desafios, torna-se imperativo buscar soluções que harmonizem a maximização da utilidade dos dados com o total respeito pela privacidade dos cidadãos. É nesse cenário que as Tecnologias de Aprimoramento da Privacidade - PETs surgem como um conjunto de ferramentas essenciais para preservar e aprimorar a privacidade e a proteção de dados pessoais. As PETs estão intrinsecamente ligadas ao conceito de privacidade desde a concepção, uma abordagem de engenharia de software e gestão estratégica que busca reduzir e mitigar os riscos de privacidade desde as fases iniciais do desenvolvimento de sistemas e serviços, por meio de controles técnicos e de governança (COUTINHO, 2025).

Entre as principais tecnologias de privacidade e medidas de mitigação recomendadas para as cidades inteligentes, destacam-se a anonimização, para que não seja possível identificar o titular, tornando-os não sujeitos às legislações de proteção de dados pessoais; pseudonimização, que mitiga a identificabilidade de um dado, mas é reversível por meio de informações adicionais mantidas separadamente; criptografia, que transforma dados legíveis em códigos, inviabilizando a interceptação e leitura não autorizada e garantindo o compartilhamento seguro; minimização de dados, que busca coletar apenas os dados relevantes e estritamente necessários para as finalidades previstas, mantendo-os armazenados somente pelo tempo indispensável; computação de borda, que processa os dados localmente e só transmite informações analíticas ou agregadas, a fim de evitar o tráfego integral de dados pessoais. Ainda, é possível utilizar metodologias de transparência e consentimento, para conscientizar a população sobre "como" e "por que" seus dados

estão sendo coletados e utilizados, oferecendo opções de participação no processo (BRASIL,2024c).

COUTINHO (2025) indica a oportunidade de se utilizar as próprias tecnologias digitais, como IoT e IA, para a proteção de dados. Este artigo tem como objetivo principal identificar e analisar as principais tecnologias de privacidade aplicadas ao contexto das cidades inteligentes, destacando a relevância da proteção de dados pessoais e detalhando o conceito e a aplicação das PETs. São apresentados exemplos de como essas ferramentas podem contribuir para um desenvolvimento urbano mais seguro e que considere a privacidade de dados, principalmente dados pessoais. O estudo considera tanto a produção científica quanto publicações governamentais e institucionais, adotando uma abordagem exploratória e qualitativa para mapear soluções tecnológicas, identificar tendências e compreender o panorama atual das estratégias de proteção da privacidade em cidades inteligentes.

2. Metodologia

A pesquisa foi conduzida por meio de estudo exploratório e qualitativo, com base em pesquisa bibliográfica. Foram consideradas três frentes principais de busca:

- a) Literatura cinzenta, totalizando 24 documentos identificados, contemplando publicações oficiais de órgãos nacionais, como o Ministério do Desenvolvimento Regional - MDR, a Autoridade Nacional de Proteção de Dados - ANPD e o Instituto Nacional de Propriedade Industrial - INPI, bem como de organizações internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico - OCDE, a Agência da União Europeia para Cibersegurança - ENISA, e o Instituto Nacional de Padrões e Tecnologia Americano - NIST.
- b) Conexões realizadas durante o Workshop sobre Capacidades em IA, realizada na Universidade de Tshingua, em Pequim, na China, nos dias 12 a 17 de maio de 2025.
- c) Literatura científica indexada, obtida na base Scopus com as palavras-chave “*smart cit*” AND “*data protection*”^{*}.

A priorização dos artigos foi realizada por meio do método Methodi Ordinatio (PAGANI, 2023). Inicialmente, foram identificados 139 artigos; 37 foram excluídos por apresentarem InOrdinatio inferior a 50, restando 102 artigos. Um artigo adicional foi removido após leitura do resumo por não aderência temática, resultando em um corpus final de 101 artigos.

A aplicação do Methodi Ordinatio permitiu selecionar os estudos mais relevantes, abrangendo publicações entre 2016 e 2025, o que possibilitou a análise de tecnologias emergentes e consolidadas para a proteção da privacidade em cidades inteligentes. Os documentos da literatura cinzenta complementaram a análise, fornecendo uma perspectiva regulatória e estratégica. Essa combinação de fontes favoreceu uma visão integrada, que inclui aspectos tecnológicos, normativos e institucionais.

A abordagem exploratória e qualitativa, aliada ao uso do Methodi Ordinatio, foi escolhida para o levantamento de tecnologias e tendências. A inclusão de literatura cinzenta ampliou o escopo da pesquisa, incorporando visões regulatórias e políticas públicas. Além disso, ferramentas de inteligência artificial generativa, como NotebookLM, ChatGPT e Manus, foram utilizadas para organização, análise de dados e triagem de informações, otimizando a identificação de relações entre soluções tecnológicas e desafios de privacidade.

3. Referencial Teórico

A urbanização acelerada e a crescente pressão sobre os recursos urbanos impulsionaram o surgimento das cidades inteligentes como um paradigma de desenvolvimento (BRASIL, 2020). Este conceito, ainda em constante evolução e passível de diversas interpretações, visa utilizar intensivamente as TICs para aprimorar a qualidade de vida dos cidadãos, otimizar a eficiência dos serviços urbanos, promover a sustentabilidade e aumentar a

resiliência dos espaços. O objetivo primordial é solucionar problemas concretos, criar oportunidades, reduzir desigualdades e melhorar o bem-estar de todas as pessoas, garantindo o uso seguro e responsável de dados e das TICs (OCDE, 2020).

A base tecnológica das cidades inteligentes é vasta, abrangendo redes de comunicação 5G, IoT, *big data*, IA, *blockchain*, drones, impressoras 3D, *gamification*, veículos inteligentes, tecnologias de nuvem e computação de borda. Essas tecnologias permitem a coleta massiva de dados com alta precisão e variedade, sendo consideradas essenciais para o funcionamento e a inovação nas cidades (FIGUEIREDO, 2022). O termo "cidade inteligente" surgiu na década de 1990, com foco inicial na integração das TICs à infraestrutura urbana, e evoluiu para uma visão mais abrangente que transcende aspectos puramente técnicos, englobando competitividade econômica, sustentabilidade ambiental e qualidade de vida geral (REZENDE, 2019).

A intensa coleta e o tratamento massivo de dados em cidades inteligentes geram preocupações significativas e diversos desafios à privacidade e à proteção dos dados pessoais dos cidadãos (OLIVEIRA, 2024). O dilema entre privacidade e eficiência é moderno, e a falta de transparência sobre o uso dos dados agrava essa questão (ARTIGO19 et al, 2024).

Entre os principais desafios e riscos identificados (BRASIL, 2024b, BRASIL, 2024c), destacam-se:

a) Vigilância e controle: a coleta indiscriminada de dados por governos e empresas pode gerar informações detalhadas, levando a um controle social excessivo e assimetria de poder. Tecnologias como o reconhecimento facial podem rastrear a população em espaços públicos, tornando-a vulnerável à arbitrariedade ou a sistemas de IA treinados com dados enviesados.

b) Uso comercial indevido e desvio de finalidade: empresas fornecedoras podem capitalizar dados mesmo oferecendo serviços gratuitos aos municípios. Casos de uso para finalidades não informadas ou em desacordo com direitos fundamentais já resultaram em condenações.

c) Dificuldade de consentimento e responsabilidade compartilhada: a complexidade e multiplicidade de finalidades de coleta de dados tornam desafiadora a obtenção de consentimento específico e informado. A responsabilidade frequentemente compartilhada entre múltiplos atores público-privados também dificulta a responsabilização.

d) Ciberataques e vulnerabilidades: a falta da priorização da segurança e privacidade no desenvolvimento das tecnologias, ataques à integridade, confidencialidade e disponibilidade dos dados, e a baixa maturidade de políticas de cibersegurança são riscos eminentes. Ciberataques e vazamentos de dados podem gerar prejuízos incalculáveis (SOARES et al, 2023).

d) Vieses e discriminação: as tecnologias não são neutras e podem incorporar vieses preconceituosos, a depender dos dados utilizados para treinamento. O uso de dados não representativos em algoritmos preditivos pode levar à discriminação racial, de gênero ou de classe, entre outros, aprofundando desigualdades sociais pré-existentes e afetando grupos vulneráveis (BRASIL, 2025).

A coleta de dados pessoais, especialmente os dados sensíveis, pode abrir precedentes graves, dependendo do contexto histórico e da forma como são tratados (SOARES et al, 2023). Portanto, a governança dos dados coletados nas cidades inteligentes precisa ser aprimorada para evitar a vulnerabilização dos direitos personalíssimos dos cidadãos.

Diante dos desafios impostos pela coleta massiva de dados em cidades inteligentes e da necessidade de conformidade com regulamentações como o Regulamento Geral de

Proteção de Dados (GDPR) na Europa, a Lei Geral de Proteção de Dados (LGPD) no Brasil, e a Lei de Proteção de Informações Pessoais na China, torna-se imperativa a adoção de soluções que conciliem a máxima utilidade das informações com a proteção da privacidade dos cidadãos (LUDGERO, 2025). Entre as abordagens para o tratamento de dados pessoais nesse contexto, destacam-se propostas de atualizações no marco legal, visando incluir disposições específicas sobre o uso de dados pelo poder público; o fortalecimento da governança, por exemplo, mediante a criação de um comitê plural composto por representantes governamentais, do setor privado, da academia, de órgãos de controle e da sociedade civil, com a missão de formular e implementar políticas de proteção de dados; o engajamento e educação da população, com incentivo à participação cidadã e à conscientização por meio de audiências públicas; e a utilização de TICs para promover o equilíbrio entre utilidade dos dados e preservação da identidade dos indivíduos, utilizando o conceito de “privacidade desde a concepção” para mitigar riscos antes de sua ocorrência (REZENDE, 2019), não se limitando ao cumprimento de normas, mas antecipando e mitigando riscos desde as fases iniciais (OECD, 2023). Assim, o avanço da digitalização, aliado à proteção dos direitos fundamentais e à evolução normativa, impulsionou o uso de Tecnologias de Aprimoramento da Privacidade (*Privacy-Enhancing Technologies* - PETs), as quais emergem como ferramentas estratégicas para enfrentar os desafios da privacidade em cidades inteligentes, com o potencial de capacitar os cidadãos e fomentar a governança colaborativa ao invés de criar um ambiente de vigilância e erosão da confiança (SUSTAINABILITY DIRECTORY, 2025).

As PETs são um conjunto de ferramentas e técnicas desenvolvidas para preservar e aprimorar a privacidade e a proteção de dados pessoais, que visam proteger a privacidade ao eliminar ou reduzir dados pessoais ou prevenir seu processamento desnecessário ou indesejado, sem comprometer a funcionalidade do sistema de informação (HANSEN et al, 2015). Estão intrinsecamente ligadas ao princípio da privacidade desde a concepção. Entre as principais PETs e medidas de mitigação recomendadas para cidades inteligentes para privacidade dos dados (BRASIL, 2024b; BRASIL, 2024c; COUTINHO, 2025), destacam-se:

a) Anonimização e pseudonimização: são técnicas que modificam dados pessoais para limitar ou impedir a identificação do titular, visando a ofuscação de dados. A anonimização altera os dados irreversivelmente, tornando impossível associá-los a um indivíduo, fazendo com que requisitos de proteção de dados pessoais deixem de se aplicar a eles. A pseudonimização mitiga a identificabilidade, mas é reversível mediante informação adicional mantida separadamente.

b) Criptografia: transforma dados legíveis em códigos, garantindo compartilhamento seguro e prevenindo acesso não autorizado.

c) Minimização de dados: consiste em coletar e tratar apenas os dados estritamente necessários para a finalidade pretendida, e armazená-los pelo tempo indispensável. O princípio da necessidade, citado em algumas legislações, busca a limitação ao tratamento mínimo necessário.

d) Computação de borda: processa dados no próprio dispositivo coletor, reduzindo o tráfego de dados pessoais completos para a rede ou nuvem e reportando apenas informações analíticas ou agregadas.

e) Dados sintéticos: dados gerados artificialmente para uso em desenvolvimento e testes de sistemas de IA, que podem atuar como PETs se usados para gerar conjuntos de dados não pessoais com utilidade similar aos reais.

f) Processamento federado e criptografia homomórfica: são técnicas que permitem análise e processamento de dados sem expor informações subjacentes.

A adoção das PETs oferece vantagens como demonstrar a privacidade por design e por padrão, cumprindo requisitos legais e as expectativas dos usuários. Elas facilitam a conformidade com o princípio da minimização de dados, proporcionam um nível adequado de segurança e minimizam os riscos de violação de dados.

Por fim, destaca-se que, embora as PETs desempenhem um papel crucial na obtenção de anonimização adequada, elas não substituem a necessidade de outras medidas para garantir o tratamento justo e transparente dos dados pessoais, exigindo uma abordagem multidisciplinar e um equilíbrio entre proteção e utilidade dos dados. A colaboração multidisciplinar é essencial para uma abordagem abrangente e eficaz (COUTINHO, 2025).

4. Resultados e discussões

Dos 101 artigos analisados, 67 (66%) apresentaram propostas de soluções para a proteção de dados, enquanto os 34 restantes (34%) tiveram caráter predominantemente analítico ou exploratório, focando em diagnósticos, desafios e lacunas existentes, sem a proposição de soluções concretas.

A Tabela 1 apresenta a distribuição dos 67 artigos que mencionam tecnologias aplicadas à proteção de dados em cidades inteligentes, evidenciando as soluções mais exploradas no período de 2016 a 2025. Observa-se que 62 artigos discutem o uso de tecnologias digitais que podem ser classificadas como PETs. Destes, 32 artigos abordam aplicações de IoT, reforçando sua centralidade no ecossistema das cidades inteligentes, especialmente para coleta e integração de dados urbanos. A IA aparece em 27 artigos, com crescente relevância a partir de 2017, destacando seu papel no processamento avançado de dados, mas também no aumento dos riscos de reidentificação, o que demanda soluções robustas de proteção. Tecnologias baseadas em *blockchain* são citadas em 13 publicações, concentradas a partir de 2020, com ênfase na rastreabilidade e transparência de transações. Apenas um artigo menciona tecnologias quânticas, o que sugere um campo emergente ainda pouco explorado.

Além disso, 5 artigos abordam mecanismos de consenso e controle, associados a estratégias de responsabilização e governança de dados, fundamentais para garantir conformidade a legislações de proteção de dados pessoais. Destaca-se também que 10 artigos propuseram soluções híbridas, combinando diferentes tecnologias para aprimorar a proteção de dados: dois combinam *blockchain* e IoT; quatro, IoT e IA; dois, *blockchain* e IA; um propõe a integração *blockchain* + IoT + IA; e outro explora IoT com computação quântica, evidenciando tendências inovadoras.

Tabela 1 – Distribuição dos artigos que mencionam tecnologias aplicadas à proteção de dados (2016–2025)

Tecnologia	Número de Artigos	Período de Publicação
Internet das Coisas – IoT	32	2016 a 2025
Inteligência Artificial - IA	27	2017 a 2025
Mecanismos de consenso ou controle	05	2020 a 2024
Blockchain	13	2020 a 2025
Tecnologias Quânticas	01	2025
TOTAL:	67	2016 a 2025

Fonte: Elaboração própria

A Tabela 2 apresenta a distribuição dos artigos que abordam desafios específicos de proteção e privacidade de dados em cidades inteligentes, categorizando-os de acordo com a natureza das soluções propostas. A categoria “segurança dos dados e cibersegurança” é a mais recorrente, com 32 artigos publicados entre 2016 e 2025, destacando soluções baseadas em IA, IoT, infraestrutura de TICs e métodos criptográficos, incluindo mecanismos de autenticação para proteção de acesso e confidencialidade. Em seguida, 23

artigos concentram-se em “anonimização e pseudonimização”, explorando principalmente *blockchain* e minimização de dados para mitigar riscos de reidentificação.

A categoria “análises federadas e distribuídas”, presente em 4 publicações a partir de 2021, foca no desenvolvimento de técnicas que viabilizam o processamento e a análise de dados sem expor informações sensíveis. Já a “responsabilização de dados”, tema de 8 artigos publicados desde 2018, trata da adoção de mecanismos de governança e compliance para garantir a conformidade com legislações de proteção de dados pessoais.

Tabela 2 – Distribuição dos artigos por desafios de proteção e privacidade de dados (2016–2025)

Desafios abarcados	Número de Artigos	Ano da Publicação
Segurança dos dados / cibersegurança	32	2016-2025
Anonimização e pseudonimização	23	2020-2025
Análises federadas e distribuídas	04	2021-2025
Responsabilização de dados	08	2018-2025
TOTAL:	67	2016-2025

Fonte: Elaboração própria

Essa distribuição evidencia uma predominância de pesquisas voltadas à segurança, mas com atenção crescente a privacidade por design e estratégias regulatórias, refletindo uma evolução do campo rumo a soluções integradas de proteção de dados.

Os dados acima corroboram com o estudo de patentes realizado pelo INPI (BRASIL, 2024a), que indica uma concentração de patentes na área de segurança de dados, aplicadas principalmente na proteção de infraestruturas críticas, sistemas de monitoramento e informações coletadas por dispositivos IoT. Elas visam resolver problemas cruciais de privacidade e proteção de dados, como violação de dados, acesso não-autorizado e garantia da integridade e confidencialidade. Também destaca o uso de tecnologias como IA, IoT, *big data* e conectividade 5G como principais tecnologias utilizadas nas cidades inteligentes e que, portanto, também introduzem complexos desafios de privacidade e proteção de dados.

4.1 Contexto brasileiro

No Brasil, a Carta Brasileira para Cidades Inteligentes - CBCI (BRASIL, 2020) propõe uma agenda pública para a transformação digital urbana, baseada em desenvolvimento sustentável e ações planejadas, inovadoras, inclusivas e em rede. Destaca-se o objetivo de estabelecer sistemas de governança de dados com transparência, segurança e privacidade. A busca por um conceito unificado de "cidade inteligente" é vista como essencial diante da complexidade digital do país. Complementam essa agenda o Plano Nacional de Internet das Coisas (BRASIL, 2019), com diretrizes para o desenvolvimento desta tecnologia no país, e o Plano Brasileiro de Inteligência Artificial, que aborda as ações estratégicas para o desenvolvimento de uma IA para o bem de todos (BRASIL, 2024d).

Nas cidades inteligentes, a coleta e o uso intensivo de dados tornam a proteção de dados pessoais fundamental. No Brasil, a privacidade é garantida pela Constituição (art. 5º, X), reforçada pela Emenda Constitucional nº 115/2022, que inclui a proteção de dados entre os direitos fundamentais. A Lei Geral de Proteção de Dados - LGPD regula o tema, protegendo a liberdade, a privacidade e o livre desenvolvimento da personalidade, mesmo sem tratar diretamente de cidades inteligentes. A lei define dado pessoal como qualquer informação que identifique ou possa identificar uma pessoa, incluindo dados sensíveis como origem racial, crença religiosa, saúde e biometria (BRASIL, 2018). Embora a LGPD não se refira especificamente às cidades inteligentes, a Autoridade Nacional de Proteção de Dados - ANPD (BRASIL, 2024b) relaciona as principais preocupações de privacidade no contexto das cidades inteligentes. Tanto dados sensíveis quanto não sensíveis exigem

proteção (DONELA, 2011), evidenciando a relação direta entre privacidade e proteção de dados no ambiente urbano digital.

A LGPD, em seu artigo 46, incorpora conceitos similares à “privacidade desde a concepção” ao exigir que os controladores de dados adotem medidas de segurança técnicas e organizacionais desde o projeto do produto ou serviço. Embora o uso de PETs em cidades inteligentes brasileiras ainda se encontre em estágio embrionário, já se observam práticas como a adoção de mecanismos de criptografia, autenticação e técnicas de anonimização, além da incorporação do princípio de “privacidade desde a concepção” em políticas públicas, por exemplo, na implantação de tecnologias de governo digital (BRASIL, 2024d). No entanto, há lacunas de informação e dados consolidados, o que dificulta uma análise sistematizada e abrangente sobre a efetividade, alcance e maturidade do uso dessas tecnologias no contexto urbano brasileiro.

4.2 Contexto timorense

No Timor-Leste, observa-se a promoção da transformação digital do país a partir dos serviços públicos. O Plano Estratégico Timor Digital 2032 visa orientar o desenvolvimento das capacidades digitais, que são fundamentais para implementar iniciativas de cidades inteligentes. O Plano aborda áreas como infraestrutura nacional e governamental, sistemas governamentais, identidade única, literacia e habilidades digitais, participação civil, investimentos do setor privado, equidade de gênero, comércio eletrônico, saúde digital, educação, agricultura e marco legislativo habilitador. Para além dos desafios ligados ao fornecimento de energia elétrica, a carência de habilidades digitais por parte dos usuários surge como um dos principais obstáculos à adoção e ao pleno funcionamento de sistemas inteligentes. Para o aperfeiçoamento da infraestrutura de conectividade, destaca-se a instalação de cabos submarinos atualmente em andamento (TATOLI, 2023).

O país ainda não possui uma legislação específica e abrangente sobre proteção de dados pessoais, embora haja indícios de uma crescente preocupação com o tema. O Decreto Lei 17/2003, que versa sobre dados estatísticos, *determina o direito à privacidade e à proteção dos dados pessoais dos cidadãos inquiridos, preservando a sua confidencialidade, em conformidade com as disposições conjugadas dos Artigos 36, 38 e 95 da Constituição timorense*; e o Plano Estratégico para Timor Leste 2011-2030 do Sector da Justiça prevê a atuação do Ministério da Justiça para criação de uma lei sobre a proteção de dados pessoais.

4.3 Contexto chinês

As cidades inteligentes na China surgiram a partir da estratégia nacional de longo prazo, que adotou o ecossistema de inovação como base para o desenvolvimento. Entre 1978 e 1985, iniciou-se a renovação científica, com a reestruturação de universidades e institutos de pesquisa. Na primeira onda (1985–1998), buscou-se tornar o sistema mais orientado ao mercado, com a criação de parques tecnológicos e estímulo ao empreendedorismo - ambiente que deu origem a empresas hoje líderes globais. A segunda onda (1998–2006) trouxe maior maturidade institucional, com avanços na governança e na consolidação de centros de pesquisa de alto nível mundial. A terceira onda (2006–2020) foi marcada pelo Plano de Médio e Longo Prazo - MLP, que lançou 16 mega-projetos estratégicos para consolidar a China como potência em inovação. Atualmente, o país fortalece sua liderança tecnológica global, integrando ciência, educação e formação de talentos.

Na década de 80, a China passou a desenvolver sistemas de informação aplicados a áreas urbanas como construção, finanças, energia e transporte. Na década de 90, destaca-se o esforço para promover a interoperabilidade, com a integração desses sistemas nos cinco níveis de governo. No final dos anos 1990, grandes projetos nas áreas de governo digital, finanças e comércio aceleraram a digitalização urbana. O MLP, a partir de 2006,

impulsionou melhorias em setores como energia, mobilidade, saneamento, educação, saúde e iluminação pública. Mais recentemente, os avanços em inteligência artificial geral têm ampliado as possibilidades de aplicação, desde o uso doméstico até simulações complexas voltadas ao planejamento urbano e nacional.

Quanto à proteção de dados pessoais, o sistema chinês adota uma abordagem ampla, que busca equilibrar privacidade individual com segurança nacional e soberania digital. O arcabouço legal é composto por leis interconectadas, como a Lei de Cibersegurança e a Lei de Segurança de Dados. A Lei de Proteção de Informações Pessoais define como dado pessoal qualquer informação relacionada a pessoa natural identificada ou identificável, excetuando-se dados anonimizados. Dentro do arcabouço legal para atendimento à legislação, destacam-se orientações técnicas publicadas pelo organismo de padronização chinês - GB, como o GB/T 45574-2025, que estabelece requisitos de segurança para o tratamento de informações pessoais sensíveis.

O estudo do INPI, que analisa os pedidos de patentes até o ano de 2022, revela que a China se posiciona como líder no desenvolvimento de tecnologias de segurança de dados para cidades inteligentes, com um número expressivo de pedidos de patentes (14.547). Os Estados Unidos (3.080 pedidos) e a Coreia do Sul (1.114 pedidos) também demonstram atividade significativa, embora em menor escala comparada à China (BRASIL, 2024a). O total de 21.354 pedidos de patentes analisados, com 68% originários da China, sublinha o foco intenso no desenvolvimento de soluções para proteger informações em ambientes urbanos conectados. Tal resultado revela um avanço expressivo, em consonância com as estratégias de desenvolvimento tecnológico e com as exigências relativas à proteção de dados pessoais no país.

5. Conclusões

Este estudo apresentou o papel das Tecnologias de Aprimoramento da Privacidade - PETs como soluções estratégicas para enfrentar os desafios de privacidade e proteção de dados nas cidades inteligentes. O avanço dessas cidades, impulsionado pela integração de tecnologias como IoT, IA e big data, apresenta um potencial transformador para a gestão urbana e a melhoria da qualidade de vida. No entanto, a coleta massiva de dados pessoais e sensíveis impõe desafios significativos à privacidade e à proteção das informações.

Por meio de uma metodologia exploratória e qualitativa, que combinou análise de literatura cinzenta de órgãos reguladores e instituições internacionais com revisão da literatura científica indexada, foi possível mapear tendências e tecnologias empregadas para equilibrar a utilidade dos dados com a salvaguarda da privacidade.

Os resultados evidenciam a emergência de um ecossistema tecnológico diversificado voltado à proteção de dados em cidades inteligentes. Tecnologias como anonimização e pseudonimização, criptografia, minimização de dados, computação de borda, dados sintéticos e processamento federado surgem como pilares para a implementação do conceito de *privacy by design* e *data protection by default*. Adicionalmente, soluções baseadas em *blockchain* mostram relevância crescente na garantia da segurança e integridade dos dados. Também ficou evidenciado que a IA deve atuar não apenas na coleta, mas também no aprimoramento da segurança e ofuscação de informações. Além disso, aplicações de IoT se apresentam como fonte de dados que exigem proteção robusta. Embora incipiente, a computação quântica desponta como uma tendência promissora, oferecendo novas abordagens para criptografia e antecipando ameaças futuras à cibersegurança.

A pesquisa também apresentou experiências de três países em diferentes estágios de desenvolvimento no que se refere a cidades inteligentes e à proteção de dados: Brasil, Timor-Leste e China. A China lidera globalmente a inovação tecnológica voltada à proteção

de dados em cidades inteligentes. O Brasil, por sua vez, encontra-se em processo de implementação de políticas públicas voltadas à modernização urbana por meio do uso de tecnologias digitais. Já o Timor-Leste está em uma fase inicial, voltada à estruturação de sua infraestrutura digital. No que diz respeito à proteção de dados pessoais, a China possui um marco regulatório que vincula esse tema à segurança nacional e à soberania digital. O Brasil conta com uma legislação robusta, cuja aplicação está em fase de amadurecimento. Já o Timor-Leste ainda não dispõe de uma legislação específica sobre o tema. Apesar das diferentes realidades, os três países demonstram esforços para equilibrar a proteção de dados pessoais com o avanço da inovação tecnológica, visando beneficiar tanto os cidadãos quanto as cidades. Nesse contexto, identificam-se oportunidades futuras de cooperação internacional, com possíveis benefícios como salto tecnológico, harmonização regulatória, desenvolvimento de capacidades e ampliação de mercados, entre outros.

Em suma, a construção de cidades inteligentes sustentáveis e centradas no cidadão requer uma abordagem integrada e proativa de privacidade e proteção de dados. As PETs, associadas a um arcabouço regulatório sólido e a uma governança de dados transparente, aliadas à participação de uma população consciente e engajada, são fundamentais para mitigar os riscos da digitalização urbana. A harmonização entre inovação tecnológica e garantia dos direitos fundamentais não constitui apenas um imperativo legal, mas também um pilar essencial para um futuro urbano mais ético, seguro e confiável.

Referências

ARTIGO 19; INTERNETLAB; LAPIN. Cidades Inteligentes e Dados Pessoais: Recomendações e Boas Práticas. São Paulo, 2022. Disponível em: <https://lapin.org.br/wp-content/uploads/2022/08/Cidades-Inteligentes-e-Dados-Pessoais-InternetLab-ARTIGO-19-e-LAPIN.pdf>

BRASIL, Presidência da República. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. Decreto nº 9.854, de 25 de junho de 2019. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Machine-to-Machine e Internet das Coisas. Diário Oficial da União: Seção 1, Brasília, DF, 26 jun. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9854.htm

BRASIL, Ministério do Desenvolvimento Regional - MDR; Ministério da Ciência, Tecnologia e Inovação - MCTI; Ministério das Comunicações; GIZ – Deutsche Gesellschaft für Internationale Zusammenarbeit. Carta Brasileira para Cidades Inteligentes: edição revisada, 2020. Brasília: MDR; MCTI; MCOM; GIZ, [s.d.]. 180 p. Disponível em: https://cartacidadesinteligentes.org.br/files/carta_brasileira_cidades_inteligentes.pdf

BRASIL, Instituto Nacional da Propriedade Industrial - INPI. Núcleo de Inteligência em Propriedade Industrial. Estudo Cidades Inteligentes. Brasília: INPI, 26 abr. 2023. Atualizado em 24 out. 2024, 2024a. Disponível em: https://www.gov.br/propriedade-intelectual/pt-br/assuntos/colegiados/grupo-tecnico-de-inteligencia-em-propriedade-industrial/estudos/estudo-nipi_cidades-inteligentes.pdf

BRASIL, Autoridade Nacional de Proteção de Dados Pessoais – ANPD. Radar Tecnológico nº1: Cidades Inteligentes, 2024b. Disponível em: www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/publicacao_radar_tecnologico_jan_2024.pdf

BRASIL, Autoridade Nacional de Proteção de Dados Pessoais – ANPD. Radar Tecnológico Inteligência Artificial Generativa. Brasília, DF: Autoridade Nacional de Proteção de Dados

(ANPD), nov. 2024c. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar_tecnologico_ia_generativa_anpd.pdf

BRASIL, Ministério da Gestão e Inovação – MGI. Guia sobre Privacidade desde a Concepção e por Padrão. Programa de Privacidade e Segurança da Informação - PPSI. Brasília, 2024d. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_privacidade_concepcao.pdf

BRASIL, Autoridade Nacional de Proteção de Dados Pessoais – ANPD. Radar Tecnológico Neurotecnologias. Brasília, DF: Autoridade Nacional de Proteção de Dados (ANPD), jun. 2025. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-4-neurotecnologias.pdf>

BRASIL. Ministério da Ciência, Tecnologia e Inovação. IA para o bem de todos; Plano Brasileiro de Inteligência Artificial (PBIA). 2024d. Disponível em https://www.cgee.org.br/documents/10195/11009772/CGEE_PBIA.PDF

CHINA, República Popular da China. Personal Information Protection Law of the People's Republic of China. 20/08/2021. Disponível em: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

COUTINHO, Tatiana. Tecnologias de Aprimoramento da Privacidade (“PETs”): Integrando princípios de privacidade por design. Lima Feigelson, 10 abr. 2025. Disponível em: <https://www.limafeigelson.com.br/blog-post/tecnologias-de-aprimoramento-da-privacidade-pets-integrando-principios-de-privacidade-por-design>

DONELA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJL], 12(2), 91–108, 2011. Disponível em: <https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315>

FIGUEIREDO, Joana Diniz de. As Smart Cities e a Privacidade: o critério legal para a anonimização de dados agregados. Anuário da Proteção de Dados, 2022. Disponível em: <https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/12/7.-Joana-Figueiredo.pdf>.

GB, China National Standards. Data Security Technology - Sensitive Personal Information Processing Security Requirements. 25/04/2025. Disponível em: https://www.gbstandards.org/GB_standard_english.asp?code=GB/T%2045574-2025

HANSEN, Marit; HOEPMAN, Jaap-Henk; JENSEN, Meiko. Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies: Methodology, Pilot Assessment, and Continuity Plan. ENISA – European Union Agency for Network and Information Security. Editor: Stefan Schiffner. [S.l.], v. 1.0, dez. 2015. Disponível em: <https://www.enisa.europa.eu/sites/default/files/publications/Readiness%20Analysis%20for%20the%20Adoption%20and%20Evolution%20of%20Privacy%20Enhancing%20Technologies.pdf>

LUDGERO, Paulo Ricardo. Proteção de Dados em Smart Cities: Desafios para a Privacidade em Cidades Inteligentes. JusBrasil, 2025. Disponível em: Proteção de Dados em Smart Cities: Desafios para a Privacidade em Cidades Inteligentes | JusBrasil

OECD, Organisation for Economic Cooperation and Development. “Emerging privacy-enhancing technologies: Current regulatory and policy approaches”, OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, 2023. Disponível em: <https://doi.org/10.1787/bf121be4-en>.

OECD, Organisation for Economic Cooperation and Development. “Sharing trustworthy AI models with privacy-enhancing technologies”, OECD Artificial Intelligence Papers, No. 38, OECD Publishing, Paris, 2025. Disponível em: <https://doi.org/10.1787/a266160b-en>.

OLIVEIRA, G. G. O impacto da IA - Inteligência Artificial no ecossistema Urbano. Uma abordagem ética. In: SEMINÁRIO EM TECNOLOGIA DA INFORMAÇÃO DE BOLSISTAS PCI DO CTI RENATO ARCHER (PCI), 14., 2024, evento virtual. Anais. Campinas: MCTI/CTI Renato Archer, 2024. p. 1-7. Disponível em: <https://www.gov.br/cti/pt-br/publicacoes/producao-cientifica/seminario-pci>.

PAGANI, Regina Negri et al. Methodi Ordinatio 2.0: revisited under statistical estimation, and presenting Flinder and RankIn. *Quality & Quantity*, v. 57, n. 5, p. 4563-4602, 2023.

PAGANI, Regina Negri. Revisão sistemática de Literatura: Methodi Ordinatio na Era da IA Generativa. Ponta Grossa: Texto e Contexto, 2024.

REZENDE, Laura Vilela Rodrigues; CRUZ-RIASCOS, Sonia Aguiar; RODRIGUES, Amanda Caroline Teles. Dados abertos em cidades inteligentes: uma análise da fronteira entre acesso e privacidade. In: IX ENCUESTRO IBÉRICO EDICIC, 2019, Barcelona. Actas, Lactud de Barcelona, 2019. Disponível em: <http://hdl.handle.net/10760/38639>

SOARES, Cinthia Gonçalves et al. As cidades inteligentes (Smart Cities) à luz da Lei Geral de Proteção de Dados. *JNT - Facit Business and Technology Journal*, [S.l.], v. 2, n. 47, p. 458-474, nov. 2023. Disponível em: <http://revistas.faculdadefacit.edu.br>

SUSTAINABILITY DIRECTORY. Privacy Enhancing Technologies in Smart Cities. Scenario: Sustainability Directory. [S.l.], 27 maio 2025. Disponível em: <https://prism.sustainability-directory.com/scenario/privacy-enhancing-technologies-in-smart-cities/>

TATOLI, Agência de Notícias de Timor-Leste. TIC Timor launch the 2023 digitalization plan in Timor-Leste. Publicado em: 02/06/2023. Disponível em: <https://en.tatoli.tl/2023/06/02/tic-timor-launch-the-2023-digitalization-platform-in-timor-leste/02/>

TIMOR-LESTE, Jornal da República. Decreto Lei Governo 17/2003. Sobre estatísticas. Disponível em: <https://www.mj.gov.tl/jornal/?q=node/1480>

TIMOR-LESTE, Ministério da Justiça. Plano Estratégico do Setor da Justiça. Publicado em: 12/02/2010. Disponível em: <https://www.mj.gov.tl/?q=node/533>

TONSAGER, Lindsey L.; PONDER, Jayne. Privacy Frameworks for Smart Cities: white paper. Ann Arbor: Mcity – University of Michigan; Covington & Burling LLP, Mar. 2023. 13 p. Disponível em: https://mcity.umich.edu/wp-content/uploads/2023/03/Privacy-Frameworks-for-Smart-Cities_White-Paper_2023.pdf