UNIVERSIDADE ESTADUAL DO PIAUÍ – UESPI
CAMPUS ALEXANDRE ALVES DE OLIVEIRA
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

JOÃO LUIZ MINEIRO ALVES

COMPUTAÇÃO UBÍQUA E OS DESAFIOS DE SEGURANÇA, PRIVACIDADE E ÉTICA NAS SMART CITIES

Parnaíba – Piauí
2025

JOÃO LUIZ MINEIRO ALVES

COMPUTAÇÃO UBÍQUA E OS DESAFIOS DE SEGURANÇA, PRIVACIDADE E ÉTICA NAS SMART CITIES

Trabalho de Conclusão de Curso (artigo) apresentado ao Curso de Bacharelado em Ciência da Computação da Universidade Estadual do Piauí, Campus Alexandre Alves de Oliveira, como requisito parcial para obtenção do grau de bacharel em Ciência da Computação.

Orientador: Prof. Dr. Átila Rabelo Lopes

Parnaíba – Piauí
2025

Computação Ubíqua e os Desafios de Segurança, Privacidade e Ética nas Smart Cities

João Luiz Mineiro Alves[1], **Atila Rabelo Lopes**[1]

[1]Coordenação do Curso de Ciência da Computação, Universidade Estadual do Piauí
Campus Prof. Alexandre Alves de Oliveira
Parnaíba, Piauí - Brasil

jluizmineiroalves@aluno.uespi.br ,atilarabelo@phb.uespi.br

Abstract. *The integration of ubiquitous computing in smart cities increases urban efficiency but raises challenges in terms of security, privacy, and ethics. This study, based on a literature review, maps the risks and solutions of this digital transformation, focusing on the vulnerabilities of IoT, Big Data, and the implications of surveillance in sectors such as public safety, mobility, health, and governance. The results highlight strategies such as Privacy by Design, Security by Design, Zero Trust architectures, and the importance of the LGPD. It is concluded that smart and humane cities depend on a balance between technological innovation and the protection of fundamental rights.*

Resumo. *A integração da computação ubíqua nas cidades inteligentes (smart cities) aumenta a eficiência urbana, mas amplia desafios de segurança, privacidade e ética. Este estudo, baseado em revisão bibliográfica, mapeia riscos e soluções dessa transformação digital, com foco em vulnerabilidades de IoT, Big Data e nas implicações da vigilância em setores como segurança pública, mobilidade, saúde e governança. Os resultados destacam estratégias como Privacy by Design, Security by Design, arquiteturas Zero Trust e a importância da LGPD. Conclui-se que cidades inteligentes e humanas dependem do equilíbrio entre inovação tecnológica e proteção dos direitos fundamentais.*

1. Introdução

A área de estudo voltada à computação ubíqua e às cidades inteligentes (smart cities) tem se mostrado de grande relevância no cenário contemporâneo, sobretudo diante do avanço acelerado das tecnologias da informação e comunicação (TICs). Segundo a formulação pioneira de Weiser [Weiser 1991], a computação ubíqua representa um novo paradigma tecnológico, no qual os recursos computacionais se integram de forma invisível ao ambiente físico, incorporando-se aos objetos e às atividades cotidianas. Essa integração possibilita uma interação fluida e natural entre o ser humano e o meio digital, tornando a tecnologia parte orgânica da vida cotidiana. Dessa forma, a computação ubíqua viabiliza a oferta de serviços personalizados, atuando de forma proativa para prover recursos e serviços adaptados ao contexto do usuário. Por outro lado, o paradigma impõe alguns desafios significativos em relação à segurança e privacidade dos dados utilizados no ambiente digital para prover adaptações ao usuário e o meio físico ao redor, que muitas vezes são coletados sem a percepção do usuário [Loureiro e Oliveira 2009].

As smart cities representam a aplicação prática dos princípios da computação ubíqua, uma vez que materializam a integração entre o mundo físico e o digital por meio

do uso intensivo das tecnologias da informação e comunicação (TICs). Fundamentadas na implementação de sistemas tecnológicos avançados como computação em nuvem, Internet das Coisas (IoT) e Big Data, as smart cities buscam promover o gerenciamento eficiente dos recursos urbanos, bem como impulsionar a sustentabilidade ambiental, a inclusão social e a melhoria da qualidade de vida [Da Cruz França 2020].

A articulação entre computação ubíqua e cidades inteligentes revela-se essencial para o desenvolvimento de ambientes urbanos mais conectados, responsivos e sustentáveis, capazes de adaptar-se dinamicamente às necessidades dos cidadãos. No entanto, essa convergência também intensifica desafios éticos e de segurança, principalmente no que se refere ao controle, uso e proteção das informações pessoais geradas e compartilhadas em larga escala [Da Cruz França 2020, Mecabô e Gueiros 2023].

A crescente implementação de tecnologias de computação ubíqua em cidades inteligentes impulsiona avanços na gestão urbana, mas simultaneamente expõe uma problemática central: a fragilidade da segurança, privacidade e ética. Vulnerabilidades técnicas, especialmente em Internet das Coisas (IoT) e Big Data, dificultam a gestão de riscos e comprometem informações sensíveis [Boghossian Torres 2017]. A complexidade da infraestrutura heterogênea e os altos custos de segurança robusta exacerbam a proteção de dados, tornando os ambientes urbanos suscetíveis a ataques e vazamentos [Mecabô e Gueiros 2023].

Esses desafios se manifestam de forma específica nos domínios urbanos críticos. Na segurança pública, a proliferação de câmeras e sensores cria vulnerabilidades que podem comprometer tanto a proteção dos cidadãos quanto sua privacidade. Na mobilidade urbana, a interconexão de sistemas de tráfego e transporte público expõe a infraestrutura a riscos de paralisação e falhas sistêmicas. No setor de saúde, a digitalização de prontuários e o uso de dispositivos de monitoramento geram dados extremamente sensíveis que, se violados, podem resultar em discriminação e fraudes. Na governança digital, a centralização de serviços e dados de cidadãos torna os governos alvos de ciberataques que podem comprometer serviços essenciais [Da Cruz França 2020, Mecabô e Gueiros 2023].

Esses riscos técnicos afetam diretamente direitos fundamentais dos cidadãos, como a privacidade, podendo resultar em vigilância excessiva e erosão da confiança nas cidades conectadas [Boghossian Torres 2017]. Portanto, a problemática central que orienta esta pesquisa é a dispersão do conhecimento sobre como os desafios de segurança e ética estão sendo efetivamente endereçados. Em vez de perguntar ”como desenvolver novas estratégias”, a questão fundamental é: Quais são os principais desafios já documentados e que soluções vêm sendo propostas para equilibrar inovação tecnológica com princípios éticos e de privacidade? A necessidade de uma análise que consolide as respostas a essa pergunta, considerando as especificidades técnicas, jurídicas e sociais [Da Cruz França 2020], é essencial para o avanço responsável e sustentável das cidades inteligentes.

O objetivo deste trabalho é investigar os principais desafios e soluções adotadas para garantir a segurança e o uso ético das informações utilizadas pelos serviços fornecidos no contexto das cidades inteligentes. A investigação parte da identificação das tecnologias que viabilizam a computação ubíqua no contexto urbano, para então analisar os riscos de segurança, privacidade e as implicações éticas decorrentes.

Especificamente, o estudo busca examinar como esses desafios se apresentam nos domínios de segurança pública, mobilidade urbana, saúde e governança digital, identificando as vulnerabilidades e dilemas éticos particulares de cada setor. O foco do estudo reside em levantar, sintetizar e discutir as estratégias, políticas e diretrizes já existentes e documentadas na literatura especializada para endereçar tais desafios, oferecendo assim um panorama consolidado do estado da arte sobre o tema.

A importância social, tecnológica e jurídica do tema reside na necessidade premente de conciliar o avanço das tecnologias de smart cities com a proteção dos direitos fundamentais dos cidadãos. A relevância desta pesquisa se amplia ao considerar os impactos específicos nos domínios urbanos essenciais.

Na segurança pública, existe a tensão entre a promessa de ambientes mais seguros e o risco de vigilância excessiva [Parini 2021], onde tecnologias de monitoramento podem comprometer a privacidade dos cidadãos. Na mobilidade urbana, a segurança de sistemas de transporte conectados afeta diretamente a segurança física e a liberdade de deslocamento da população [Da Cruz França 2020]. No setor de saúde, a criticidade dos dados pessoais exige diretrizes claras para proteger a confidencialidade e permitir inovações que salvam vidas. Na governança digital, a confiança dos cidadãos depende da capacidade do Estado de proteger dados e utilizá-los de forma ética [Mecabô e Gueiros 2023, Boghossian Torres 2017]. A ausência de diretrizes claras e a falta de compreensão sobre os impactos da computação ubíqua podem levar a cenários de vigilância excessiva [Parini 2021], discriminação e perda de autonomia individual, tornando esta pesquisa crucial para o desenvolvimento de cidades verdadeiramente inteligentes e humanas.

O presente trabalho foi desenvolvido com base em uma abordagem metodológica qualitativa e exploratória, fundamentada em um estudo bibliográfico da literatura. A pesquisa abrangeu a análise de artigos científicos, relatórios técnicos, documentos regulatórios e publicações especializadas para mapear os desafios de segurança, privacidade e ética em smart cities.

O escopo da análise foi delimitado a quatro domínios centrais de serviços urbanos: segurança pública, mobilidade urbana, saúde e governança digital. A análise do conteúdo foi conduzida para identificar, categorizar e sintetizar as principais vulnerabilidades, os dilemas éticos recorrentes e as soluções de mitigação já propostas na literatura para cada um desses domínios. Dessa forma, o estudo culmina em um panorama consolidado do estado da arte, oferecendo uma síntese do conhecimento atual sobre o tema.

Este trabalho foi estruturado em cinco capítulos, além desta introdução. O segundo capítulo, Fundamentação Teórica, estabelece as bases conceituais sobre Computação Ubíqua, Cidades Inteligentes e os pilares de segurança, privacidade e ética. O terceiro capítulo detalha a Metodologia adotada, descrevendo os procedimentos de pesquisa e análise. O quarto capítulo, Análise e Discussão, constitui o cerne da pesquisa, onde são examinadas as tecnologias, os desafios e as propostas de mitigação. Por fim, o quinto capítulo apresenta as Considerações Finais, sintetizando os resultados e apontando direções para trabalhos futuros.

2. Fundamentação Teórica

Nesta seção, serão abordados os conceitos fundamentais que sustentam a presente pesquisa, proporcionando uma base teórica sólida para a compreensão dos desafios e soluções relacionados à ética e segurança em cidades inteligentes. Serão explorados temas como a Computação Ubíqua, o conceito de Smart Cities, aspectos de Segurança em Ambientes Ubíquos, questões de Privacidade e as Implicações Éticas decorrentes da integração tecnológica no contexto urbano. O objetivo é contextualizar o leitor com os pilares teóricos necessários para a análise crítica dos fenômenos estudados.

2.1. Computação Ubíqua

A Computação Ubíqua, também conhecida como Ubicomp, representa um paradigma tecnológico visionário que transcende a interação tradicional entre humanos e computadores. Concebida por Mark Weiser no final da década de 1980 e popularizada em seu artigo seminal de 1991 na Scientific American, a Ubicomp propõe um futuro onde a tecnologia se integra de forma tão harmoniosa ao ambiente que se torna praticamente invisível e onipresente [Weiser 1991]. Weiser, enquanto cientista-chefe no Xerox PARC, imaginou um mundo onde dispositivos computacionais estariam embutidos em objetos cotidianos, permitindo que as pessoas interagissem com a informação e os serviços de maneira natural e intuitiva, sem a necessidade de focar explicitamente na máquina [Gray 2024].

Desde sua concepção, a visão de Weiser tem evoluído significativamente, impulsionada pelos avanços em diversas áreas da tecnologia. Inicialmente focada em pequenos dispositivos como tabs, pads e boards, a Computação Ubíqua expandiu-se para englobar uma vasta gama de tecnologias que hoje permeiam o ambiente urbano. Essa evolução é particularmente evidente no contexto das Smart Cities, onde a Ubicomp se manifesta na forma de infraestruturas conectadas e serviços inteligentes que visam otimizar a vida urbana[Ali et al. 2023]. A transição de computadores de mesa para dispositivos móveis e, posteriormente, para ambientes inteligentes, reflete a concretização progressiva do ideal ubíquo, conforme ilustrado na Figura 1, que demonstra a evolução da computação desde os mainframes até a era da nuvem e da Ubicomp.

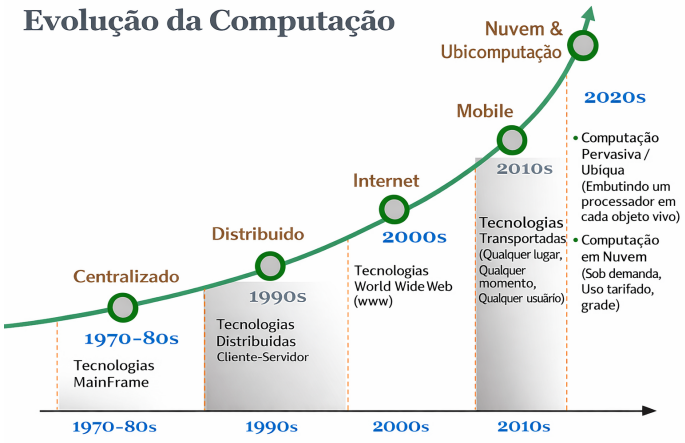

Figura 1. Evolução projetada da computação desde mainframes (1970-80s) até computação ubíqua e em nuvem (2020s). Fonte: Sedani e Doshi (2015).

As tecnologias que viabilizam a Computação Ubíqua no contexto urbano são diversas e interconectadas. A Internet das Coisas (IoT) desempenha um papel central,

permitindo que bilhões de dispositivos físicos coletem e troquem dados, desde sensores de tráfego e qualidade do ar até câmeras de segurança e medidores inteligentes. A Inteligência Artificial (IA) é fundamental para processar e analisar essa vasta quantidade de dados, transformando-os em informações acionáveis para a gestão urbana e a personalização de serviços [Ali et al. 2023]. Além disso, a computação em nuvem oferece a infraestrutura escalável necessária para o armazenamento e processamento de dados em larga escala, enquanto o Edge Computing aproxima o poder computacional da fonte de dados, reduzindo a latência e otimizando a resposta em tempo real, crucial para aplicações urbanas críticas [Khan et al. 2020].

Outras tecnologias essenciais incluem sensores de diversos tipos (temperatura, umidade, movimento, luminosidade, etc.), que atuam como os olhos e ouvidos do ambiente ubíquo, coletando informações do mundo físico. A integração desses componentes permite a criação de ecossistemas inteligentes que respondem dinamicamente às necessidades dos cidadãos e da infraestrutura urbana [Araujo 2003]. A interconexão e a capacidade de processamento distribuído dessas tecnologias são a espinha dorsal da Computação Ubíqua, transformando o ambiente em uma interface inteligente e responsiva [Lopes 2017]. A Figura 2 apresenta um modelo da arquitetura tecnológica que integra essas diferentes camadas, desde os sensores até os serviços.

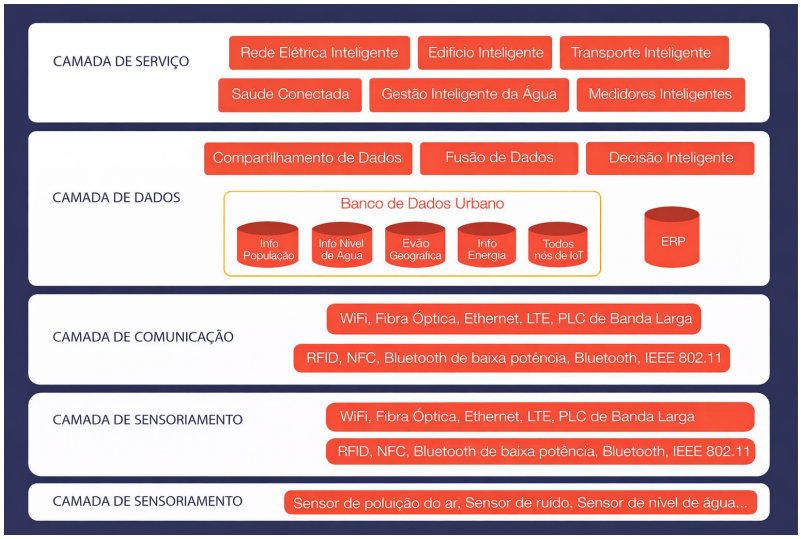

Figura 2. Arquitetura tecnológica de computação ubíqua em Smart Cities, integrando IoT, computação em nuvem e edge computing. Adaptado de Rathore et al. (2016).

A evolução da Computação Ubíqua para o contexto urbano é um reflexo direto da crescente digitalização das cidades. Onde antes a tecnologia era confinada a dispositivos específicos, hoje ela se espalha por toda a malha urbana, desde sistemas de transporte inteligentes até redes de energia otimizadas e serviços de saúde conectados [Rapôso 2025]. Essa integração profunda visa não apenas a eficiência operacional, mas também a melhoria da qualidade de vida dos habitantes, a sustentabilidade ambiental e a segurança pública. No entanto, essa onipresença tecnológica também levanta questões complexas sobre segurança, privacidade e ética, que serão exploradas nas seções subsequentes [Khan et al. 2020].

2.2. Smart Cities

O conceito de Smart Cities, ou Cidades Inteligentes, emerge como uma resposta à crescente urbanização e à necessidade de gerenciar recursos de forma mais eficiente, sustentável e inclusiva. Uma Smart City pode ser definida como um ambiente urbano que utiliza tecnologias da informação e comunicação (TICs), como a Internet das Coisas (IoT), Big Data, Inteligência Artificial (IA) e computação em nuvem, para melhorar a qualidade de vida de seus cidadãos, otimizar serviços urbanos e promover o desenvolvimento econômico e a sustentabilidade ambiental [Syed et al. 2021]. A União Europeia, por exemplo, destaca que o conceito se baseia na interação entre sistemas e pessoas, utilizando energia, materiais e serviços de forma integrada [Abadía et al. 2022].

Os modelos de Cidades Inteligentes geralmente compartilham um foco em seis eixos principais: economia, mobilidade, meio ambiente, qualidade de vida, governança e pessoas [Abadía et al. 2022]. Esses eixos representam as diferentes dimensões em que a tecnologia pode ser aplicada para transformar a cidade. A governança inteligente, por exemplo, envolve a participação cidadã e a transparência na gestão pública, enquanto a mobilidade inteligente busca otimizar o transporte e reduzir o congestionamento [Whaiduzzaman et al. 2022]. A implementação de soluções tecnológicas nesses eixos visa criar um ecossistema urbano mais resiliente e adaptável às mudanças. Esses eixos se desdobram nas seis dimensões fundamentais de uma Cidade Inteligente, detalhadas na Figura 3.

Figura 3. As seis dimensões fundamentais de uma Smart City: Economia, Mobilidade, Meio Ambiente, Pessoas, Qualidade de Vida e Governança. Adaptado de Giffinger (2007).

Diversos exemplos de Smart Cities ao redor do mundo ilustram a aplicação desses conceitos. Singapura é frequentemente citada como um modelo global, com iniciativas que abrangem desde transporte autônomo até sistemas avançados de monitoramento ambiental e de saúde. Outras cidades como Hong Kong, Zurique e Nova Iorque também se destacam por suas inovações em diferentes setores [Whaiduzzaman et al. 2022]. No

Brasil, cidades como Curitiba têm ganhado reconhecimento internacional, sendo eleita a Cidade Mais Inteligente do Mundo em 2023, devido a projetos que incluem iluminação inteligente e gestão urbana baseada em dados. Recife também se posiciona como uma cidade inteligente no cenário nacional, especialmente em conectividade [Cities 2025].

A arquitetura tecnológica de uma Smart City é complexa e envolve múltiplas camadas de infraestrutura. No nível mais básico, há uma vasta rede de sensores e dispositivos IoT que coletam dados em tempo real sobre o ambiente urbano [Syed et al. 2021]. Esses dados são transmitidos para plataformas de Big Data e computação em nuvem, onde são processados e analisados com o auxílio de algoritmos de Inteligência Artificial [Khan et al. 2020]. A partir dessa análise, são gerados insights que alimentam sistemas de gestão urbana, aplicativos para cidadãos e serviços inteligentes. A conectividade robusta, muitas vezes baseada em redes 5G, é fundamental para garantir a comunicação eficiente entre todos esses componentes [Abadía et al. 2022]. A Figura 4 ilustra como essas partes se organizam em uma arquitetura de camadas, demonstrando a integração entre sensores, comunicação, processamento de dados e serviços.

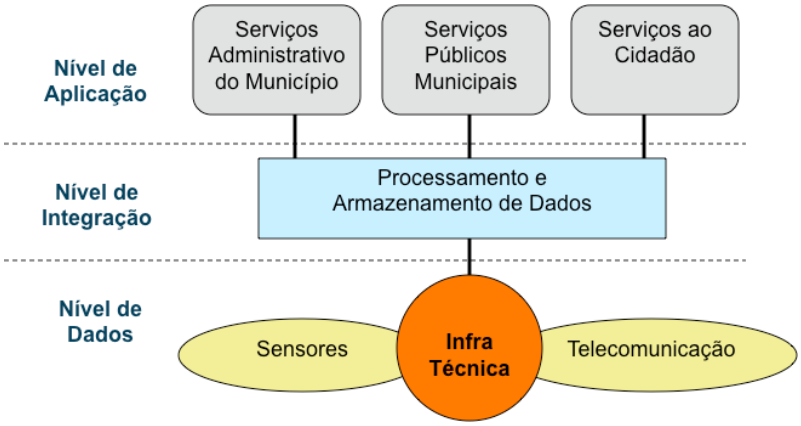

Figura 4. Arquitetura em camadas de uma Smart City, mostrando a integração entre camada de serviços, processamento de dados, comunicação e sensores IoT. Fonte: ACRJ (2017).

A implementação bem-sucedida de uma Smart City requer uma abordagem holística que transcende a mera infraestrutura tecnológica. O ecossistema urbano inteligente envolve a colaboração integrada entre o setor público, privado e a academia, além da participação ativa dos cidadãos [Bernardi et al. 2020]. Essa integração multissetorial, aliada à consideração de aspectos sociais, econômicos e ambientais, visa criar cidades que sejam não apenas tecnologicamente avançadas, mas também humanas e sustentáveis [JAI 2016].

2.3. Segurança em Ambientes Ubíquos

A onipresença da Computação Ubíqua e a proliferação de Smart Cities, embora tragam inúmeros benefícios, também introduzem um conjunto complexo de desafios de segurança. A interconexão massiva de dispositivos, sistemas e dados cria uma superfície de ataque expandida, tornando os ambientes urbanos inteligentes alvos potenciais para diversas ameaças cibernéticas [Hamid et al. 2019]. A segurança em ambientes ubíquos é, portanto, uma preocupação crítica que exige atenção contínua e estratégias robustas.

As vulnerabilidades técnicas são particularmente acentuadas em tecnologias como a Internet das Coisas (IoT) e o Big Data. Dispositivos IoT, muitas vezes projetados com foco em funcionalidade e baixo custo, podem apresentar falhas de segurança inerentes, como senhas padrão fracas, falta de criptografia, interfaces de gerenciamento inseguras e ausência de mecanismos de atualização de firmware [Hamid et al. 2019, Leite 2019], assim como demonstrado na figura 5. A heterogeneidade desses dispositivos e a dificuldade em aplicar patches de segurança de forma consistente aumentam a exposição a ataques. No contexto do Big Data, a vasta quantidade de informações coletadas e armazenadas, muitas vezes de natureza sensível, torna-se um alvo atraente para cibercriminosos, com riscos de vazamento de dados e comprometimento da integridade das informações [Santos e Freitas 2016].

Figura 5. As principais vulnerabilidades em dispositivos IoT e suas características. Adaptado de Nagaraj (2025).

Os ciberataques em infraestrutura crítica representam uma das maiores ameaças para as Smart Cities. Sistemas de controle industrial (ICS) e sistemas de supervisão e aquisição de dados (SCADA) que gerenciam serviços essenciais como energia, água, transporte e saúde podem ser alvos de ataques sofisticados [Hamid et al. 2019]. Ataques como negação de serviço (DDoS), ransomware, interceptação de dados e sequestro de dispositivos podem paralisar serviços urbanos vitais, causar danos financeiros significativos e até mesmo colocar vidas em risco [Hamid et al. 2019, Cui et al. 2018]. A interconexão entre sistemas de tecnologia da informação (TI) e tecnologia operacional (TO) nas cidades inteligentes amplifica essas vulnerabilidades, criando pontos de entrada para ataques que podem se propagar rapidamente [CISA 2023].

A gestão de riscos em ambientes ubíquos é um processo contínuo que envolve a identificação, avaliação e mitigação de ameaças. Dada a complexidade e a dinâmica das Smart Cities, as estratégias de segurança devem ser proativas e adaptáveis. Isso inclui

a implementação de arquiteturas de segurança robustas, como a Arquitetura Zero Trust, que assume que nenhuma entidade, interna ou externa, é confiável por padrão. Outras medidas incluem a detecção e resposta a endpoints (EDR), detecção de ameaças baseada em IA, gerenciamento de patches e planos de resposta a incidentes [Cui et al. 2018]. O comprometimento de informações sensíveis, como dados pessoais de cidadãos, registros de saúde ou padrões de mobilidade, pode levar a sérias violações de privacidade e perda de confiança pública, exigindo a implementação de controles rigorosos de acesso e criptografia [Ijaz et al. 2016].

Em suma, a segurança em ambientes ubíquos não é apenas uma questão técnica, mas também organizacional e política. Requer uma abordagem multifacetada que combine tecnologias avançadas de cibersegurança com políticas claras, treinamento de pessoal e colaboração entre todas as partes interessadas para proteger a infraestrutura e os dados das Smart Cities [Ijaz et al. 2016].

2.4. Privacidade

A privacidade em Smart Cities é uma preocupação central, dada a vasta quantidade de dados pessoais e sensíveis que são coletados, processados e compartilhados por meio das tecnologias ubíquas [Al-Turjman et al. 2022]. A interconexão de dispositivos IoT, câmeras de vigilância, sensores de tráfego e sistemas de governança digital gera um volume sem precedentes de informações sobre os cidadãos, seus hábitos e seus movimentos, levantando questões significativas sobre a proteção desses dados e os direitos individuais [Daoudagh et al. 2021].

Os tipos de dados coletados em ambientes urbanos inteligentes são extremamente variados. Incluem dados de localização de dispositivos móveis, registros de câmeras de segurança, informações de sensores ambientais (qualidade do ar, ruído), dados de consumo de energia e água, informações de transporte público e até mesmo dados biométricos em alguns contextos [Daoudagh et al. 2021, Hernandez-Ramos et al. 2021]. Essa coleta massiva, embora possa ser utilizada para otimizar serviços e melhorar a segurança, também pode ser empregada para fins de vigilância e perfilamento, muitas vezes sem o consentimento explícito ou o conhecimento dos indivíduos [Hernandez-Ramos et al. 2021].

Os riscos de vigilância e perfilamento são inerentes à arquitetura das Smart Cities. A capacidade de correlacionar diferentes fontes de dados permite a criação de perfis detalhados dos cidadãos, que podem ser usados para monitorar comportamentos, prever ações e até mesmo influenciar decisões [Pramanik et al. 2023]. A vigilância excessiva pode levar à erosão da confiança pública, à restrição da liberdade individual e à potencial discriminação algorítmica, onde decisões automatizadas podem afetar negativamente grupos específicos da população [Daoudagh et al. 2021, Pramanik et al. 2023]. A falta de transparência sobre como os dados são coletados, usados e protegidos agrava esses riscos, transformando cidades inteligentes em ambientes de vigilância [Moura e Silva 2019].

Para mitigar esses riscos, diversas normas e legislações aplicáveis têm sido desenvolvidas globalmente. A Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia são exemplos proeminentes de marcos legais que estabelecem direitos aos titulares de dados e obrigações às organizações que os coletam e processam [Neto 2023]. Ambas as legislações enfa-

tizam princípios como a finalidade, adequação, necessidade, transparência, segurança e prestação de contas no tratamento de dados pessoais. Elas exigem consentimento explícito para a coleta de dados, garantem o direito de acesso, retificação e exclusão, e impõem sanções significativas em caso de não conformidade [Bernardi et al. 2020].

Além das legislações, normas técnicas como a ISO/IEC 27001 desempenham um papel crucial na gestão da segurança da informação e, consequentemente, na proteção da privacidade. A ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI) [Soares e Aquino 2023]. Embora não seja específica para privacidade, a implementação de um SGSI robusto conforme a ISO/IEC 27001 fornece uma estrutura para proteger a confidencialidade, integridade e disponibilidade dos dados, o que é fundamental para a privacidade em Smart Cities [Soares e Aquino 2023]. A adoção dessas normas e legislações é essencial para construir a confiança dos cidadãos e garantir que o desenvolvimento das cidades inteligentes seja feito de forma ética e respeitosa aos direitos fundamentais [JAI 2016].

2.5. Ética

A dimensão ética nas Smart Cities é tão crucial quanto às inovações tecnológicas e as salvaguardas de segurança e privacidade. A integração pervasiva de tecnologias digitais no tecido urbano levanta questões morais complexas sobre o uso do poder, a equidade, a justiça e o respeito aos direitos humanos no ambiente conectado. A ética em cidades inteligentes busca garantir que o avanço tecnológico sirva ao bem comum e não crie novas formas de exclusão ou controle social [Ziosi et al. 2022].

A transparência e responsabilidade no uso de dados são pilares fundamentais para uma Smart City ética. Os cidadãos têm o direito de saber quais dados estão sendo coletados, por que estão sendo coletados, como estão sendo usados e quem tem acesso a eles [König 2021]. A falta de transparência pode minar a confiança pública e levar a percepções de vigilância e manipulação. A responsabilidade, por sua vez, exige que as entidades que coletam e processam dados sejam responsabilizadas por suas ações, especialmente em caso de uso indevido ou violações de segurança [König 2021]. Isso inclui a necessidade de regulamentar o uso de algoritmos para promover a equidade e evitar a discriminação algorítmica [Fonseca 2023].

O consentimento informado em ambientes pervasivos apresenta um desafio particular. Em um cenário onde a tecnologia é onipresente e muitas vezes invisível, obter o consentimento explícito e significativo dos cidadãos para a coleta e uso de seus dados pode ser complexo [Carreño-Dueñas 2016]. O modelo tradicional de consentimento, baseado em termos de serviço longos e complexos, é inadequado para a dinâmica das Smart Cities. É necessário desenvolver abordagens mais intuitivas e granulares para o consentimento, que permitam aos indivíduos controlar suas informações de forma eficaz, sem comprometer a funcionalidade dos serviços urbanos [Scott 2019].

As implicações éticas decorrentes da integração tecnológica são vastas e multifacetadas. Elas incluem o potencial para controle social através da vigilância constante, a discriminação algorítmica que pode perpetuar ou exacerbar desigualdades sociais, e os impactos na equidade urbana, onde o acesso e os benefícios das tecnologias inteligentes podem não ser distribuídos de forma justa entre todos os habitantes

[Pramanik et al. 2023, Ziosi et al. 2022]. A tomada de decisões automatizada, por exemplo, pode levar a resultados injustos se os algoritmos forem treinados com dados enviesados ou se não houver um mecanismo de revisão humana [InternetLab 2022].

Para enfrentar esses desafios, é essencial que as Smart Cities adotem um design ético de sistemas, onde as considerações éticas são incorporadas desde as fases iniciais de desenvolvimento tecnológico [Mondragon-Barrios 2009]. Isso envolve a criação de diretrizes claras, a promoção de debates públicos sobre o uso da tecnologia e a participação ativa da população na definição de políticas e na implementação de soluções [Dialnet 2009]. O objetivo é alinhar a inovação tecnológica com os direitos humanos e os valores democráticos, garantindo que as cidades inteligentes sejam verdadeiramente humanas e justas [Scielo 2014].

3. Metodologia

Esta seção detalha a abordagem metodológica adotada para a realização deste trabalho, descrevendo o tipo de pesquisa, os procedimentos empregados para a coleta e análise de dados, e as técnicas utilizadas para alcançar os objetivos propostos. A pesquisa foi conduzida com o apoio de ferramentas de inteligência artificial para otimizar a identificação e seleção de artigos científicos relevantes, bem como para facilitar a tradução de publicações em idiomas diversos, garantindo acesso amplo à literatura especializada. A escolha da metodologia, incluindo o uso estratégico de tecnologias de IA, visa garantir a robustez e a validade dos resultados obtidos, fornecendo um caminho claro e replicável para a investigação.

3.1. Tipo de Pesquisa

O presente estudo caracteriza-se como uma pesquisa qualitativa e exploratória, fundamentada em um estudo bibliográfico da literatura. A natureza qualitativa da pesquisa permite uma compreensão aprofundada dos fenômenos complexos relacionados à ética e segurança em cidades inteligentes, focando na interpretação de dados não numéricos e na identificação de padrões e significados em contextos específicos. A abordagem exploratória é justificada pela necessidade de investigar um tema ainda em desenvolvimento e com múltiplas facetas, buscando familiarizar-se com o problema e construir hipóteses, em vez de testá-las. O estudo bibliográfico da literatura é a técnica central empregada, pois permite a identificação, seleção, avaliação e síntese de toda a pesquisa relevante disponível sobre o tema. Este método oferece uma visão abrangente e imparcial do estado da arte, minimizando vieses e fornecendo uma base sólida para a análise crítica dos desafios e soluções existentes.

3.2. Procedimentos

Os procedimentos metodológicos foram estruturados em etapas sequenciais, visando a coleta e análise sistemática das informações:

3.2.1. Coleta de Dados

A coleta de dados foi realizada por meio de uma revisão bibliográfica, com o objetivo de identificar, selecionar e analisar artigos científicos, relatórios técnicos, documentos

regulatórios e publicações especializadas que abordassem a intersecção entre Computação Ubíqua, Smart Cities, Segurança, Privacidade e Ética. Ressalta-se que, embora tenha sido adotada uma abordagem sistemática na busca e seleção das fontes, o processo não seguiu todos os protocolos rigorosos de uma revisão sistemática formal, como a avaliação de qualidade metodológica ou a extração de dados padronizada.

O processo de busca utilizou uma estratégia multifacetada. O Google Scholar foi empregado como ferramenta principal para a busca exploratória e ampla, devido à sua extensa indexação que abrange diversas fontes, incluindo periódicos, anais de congresso, teses e dissertações. As bases de dados IEEE Xplore e ACM Digital Library foram utilizadas como fontes especializadas para buscas focadas, garantindo o acesso a publicações de alto impacto e revisadas por pares nas áreas de engenharia e ciência da computação. Adicionalmente, foram examinados relatórios técnicos de organizações como o IDB (Banco Interamericano de Desenvolvimento), a CISA (Cybersecurity and Infrastructure Security Agency), e documentos legais e regulatórios, como a LGPD e a GDPR.

As strings de pesquisa foram formuladas combinando termos-chave em português e inglês, utilizando operadores booleanos (AND/OR) para refinar os resultados. As strings de pesquisa utilizadas incluíram os termos: ”Smart Cities”, ”Segurança”, ”Privacidade”, ”Ubiquitous Computing”, ”Ethical Implications”, ”Discriminação Algorítmica”, ”Gestão Urbana”, ”IoT Vulnerabilities”.

O processo de busca inicial retornou um volume significativo de publicações, indicando a relevância e a atualidade do tema. A Tabela 1 sumariza a contagem de artigos encontrados para cada combinação de strings de busca nas bases de dados consultadas. Os valores elevados observados no Google Scholar refletem sua cobertura mais ampla, enquanto as bases IEEE Xplore e ACM Digital Library apresentam resultados mais focados em suas áreas de especialização.

Tabela 1. Resultados Quantitativos da Busca nas Bases de Dados

String de Busca	IEEE Xplore	ACM Digital Library	Google Scholar
Smart Cities, Segurança e Privacidade	1.585	2.268	230.000
Computação Ubíqua e Ética	102	1.443	4.270
Vulnerabilidades IoT	300	917	1.590
Big Data e Privacidade	327	948	138.000
Ataques Cibernéticos / Discriminação	2.072	1.306	892
Frameworks de Segurança / Edge	528	3.103	4.680

3.2.2. Critérios de Seleção

Para garantir a relevância e a qualidade do material, os seguintes critérios de seleção foram aplicados:

Tabela 2. Critérios de Inclusão e Exclusão da Revisão Bibliográfica

Critério	Descrição
Inclusão Temática	Intersecção entre Computação Ubíqua, Smart Cities, Segurança, Privacidade e Ética.
Natureza da Fonte	Artigos científicos (periódicos e anais de congresso), relatórios técnicos e documentos legais.
Atualidade	Publicações dos últimos 5 a 10 anos, exceto trabalhos seminais.
Idioma	Português e Inglês.
Excluir trabalhos duplicados	Remoção de trabalhos duplicados identificados em múltiplas bases de dados.

A aplicação desses critérios ao volume inicial de publicações identificadas resultou na seleção de 36 trabalhos para compor a revisão bibliográfica final. A análise da origem desses trabalhos revela que, embora o Google Scholar tenha sido a principal porta de entrada para a descoberta da maioria dos artigos, a distribuição por fonte primária de publicação é diversificada. Do total selecionado, 6 artigos (16,7%) são publicações da IEEE e da ACM, 14 artigos (38,9%) são de outros periódicos e conferências internacionais, e os 16 trabalhos restantes (44,4%) são de fontes complementares, incluindo literatura brasileira (teses, dissertações e anais de congressos), relatórios técnicos e documentos regulatórios. Essa diversidade de fontes garante que o estudo reflita tanto o estado da arte internacional quanto o contexto específico brasileiro.

3.2.3. Delimitação do Escopo

Para garantir a profundidade da análise, o escopo da pesquisa foi delimitado a quatro domínios centrais de serviços urbanos: segurança pública, mobilidade urbana, saúde e governança digital. Essa delimitação permitiu um foco específico nas intersecções entre computação ubíqua, smart cities, segurança, privacidade e ética dentro de setores críticos para a vida urbana.

3.2.4. Análise de Conteúdo

A análise de conteúdo foi a técnica principal utilizada para processar os dados coletados. Esta etapa envolveu a identificação, categorização e síntese de:

- Vulnerabilidades: Falhas e pontos fracos técnicos e operacionais em sistemas de computação ubíqua e infraestruturas de smart cities que podem ser explorados por agentes mal-intencionados.
- Dilemas Éticos: Questões morais e sociais complexas decorrentes da implementação de tecnologias inteligentes, como vigilância, privacidade, discriminação algorítmica e autonomia individual.
- Soluções de Mitigação: Estratégias, políticas, diretrizes e tecnologias propostas ou implementadas para endereçar as vulnerabilidades de segurança e os dilemas éticos identificados.

Cada documento selecionado foi lido e codificado, com a extração de trechos relevantes que abordavam esses três eixos temáticos. A categorização foi realizada de forma iterativa, permitindo a emergência de temas e subtemas que refletem o estado da arte e as lacunas existentes na literatura. A síntese final resultou em um panorama consolidado do conhecimento atual sobre a ética e segurança em cidades inteligentes, conforme apresentado nos capítulos anteriores e subsequentes deste trabalho.

4. Análise e Discussão

Esta seção apresenta uma análise integrada dos principais desafios e soluções no campo da ética e segurança em cidades inteligentes (Smart Cities), conforme mapeado pela revisão bibliográfica sistemática. A discussão segue uma estrutura narrativa que parte das tecnologias habilitadoras, passa pelos riscos que elas introduzem (segurança, privacidade e ética), e culmina nas estratégias de mitigação propostas pela literatura. O objetivo é demonstrar como esses elementos se inter-relacionam, fornecendo um panorama consolidado do estado da arte sobre o tema.

4.1. Tecnologias Habilitadoras e Seus Desafios Intrínsecos

As Smart Cities são viabilizadas por um conjunto interconectado de tecnologias de computação ubíqua que transformam a gestão urbana e a vida dos cidadãos. Porém, cada tecnologia introduz desafios específicos de segurança, privacidade e ética que precisam ser compreendidos e endereçados de forma integrada.

4.1.1. Plataformas IoT: Capacidades e Vulnerabilidades

As Plataformas de Internet das Coisas (IoT) são o coração da infraestrutura de dados das Smart Cities. Elas atuam como middleware, conectando uma vasta rede de sensores e dispositivos, coletando, processando e analisando dados em tempo real [Syed et al. 2021]. Plataformas como Cisco Kinetic, Microsoft Azure e AWS IoT Core oferecem a escalabilidade e a capacidade de processamento necessárias para gerenciar o volume massivo de informações geradas no ambiente urbano [Khan et al. 2020]. Elas permitem o gerenciamento remoto de ativos, como iluminação pública e medidores inteligentes, e fornecem insights utilizáveis para a gestão urbana, como a otimização de recursos e a manutenção preditiva [Abadía et al. 2022].

Porém, essa capacidade de coleta e processamento massivo de dados introduz desafios significativos. Os dispositivos IoT são frequentemente o elo mais fraco na cadeia de segurança das Smart Cities [Ijaz et al. 2016]. As vulnerabilidades são inerentes à sua concepção: muitos dispositivos são projetados com foco em funcionalidade e baixo custo, negligenciando mecanismos de segurança robustos como criptografia e autenticação forte [Al-Turjman et al. 2022]. A manutenção de senhas de fábrica ou a ausência de mecanismos de atualização de firmware tornam esses dispositivos alvos fáceis para invasores [Daoudagh et al. 2021]. Além disso, a vasta diversidade de dispositivos e fabricantes dificulta a aplicação consistente de patches de segurança e a gestão centralizada de riscos, aumentando a exposição a ataques [Daoudagh et al. 2021].

A escolha da plataforma IoT é crucial, pois deve garantir a interoperabilidade, a escalabilidade e, principalmente, a segurança dos dados [Bernardi et al. 2020]. Essas

vulnerabilidades em dispositivos IoT criam pontos de entrada para ataques cibernéticos sofisticados que podem comprometer toda a infraestrutura urbana.

4.1.2. Sistemas de Vigilância e Monitoramento: Segurança vs. Privacidade

A segurança pública e a gestão de tráfego são domínios que se beneficiam intensamente dos Sistemas de Vigilância e Monitoramento baseados em tecnologias ubíquas. Câmeras de alta resolução, sensores de tráfego e reconhecimento facial são integrados a Centros de Operações Urbanas (COUs). Esses sistemas utilizam a análise de vídeo inteligente para identificar comportamentos suspeitos em tempo real [JAI 2016], monitorar o fluxo de veículos e pedestres para otimizar o tráfego [Hamid et al. 2019], e gerar alertas automáticos para as autoridades em situações de emergência [Hamid et al. 2019].

Embora eficazes na prevenção de crimes e na melhoria da resposta a incidentes, a onipresença desses sistemas intensifica um dilema fundamental: a tensão entre segurança pública e privacidade individual. A infraestrutura ubíqua coleta dados de localização, padrões de mobilidade e interações sociais, muitas vezes sem a percepção ou o consentimento explícito e significativo dos cidadãos [Hernandez-Ramos et al. 2021]. O modelo tradicional de consentimento, baseado em termos de serviço longos e complexos, é inadequado para o ambiente pervasivo das Smart Cities, onde o consentimento deveria ser contextual e granular [Hernandez-Ramos et al. 2021]. A falta de transparência sobre quais dados são coletados e como são utilizados mina a confiança pública e viola princípios de proteção de dados como a LGPD e a GDPR [Pramanik et al. 2023].

4.1.3. Inteligência Artificial: Otimização e Discriminação

A Inteligência Artificial (IA) é a camada de processamento que transforma os dados brutos coletados pela IoT em ações e decisões inteligentes. A IA é aplicada em diversas áreas da gestão urbana: otimização de tráfego através de algoritmos que ajustam semáforos e rotas em tempo real para reduzir congestionamentos [Santos e Freitas 2016]; previsão de demanda com modelos preditivos que auxiliam na gestão de energia, água e resíduos, antecipando picos de consumo [Hamid et al. 2019]; e segurança pública com sistemas que analisam grandes volumes de dados de câmeras e sensores para prever áreas de risco e alocar recursos policiais de forma mais eficiente [Hamid et al. 2019].

A eficácia da IA depende fundamentalmente da qualidade e da imparcialidade dos dados de treinamento, sendo um vetor de preocupação quanto à discriminação algorítmica e à equidade urbana [Cui et al. 2018]. Algoritmos de IA utilizados em sistemas de segurança, concessão de crédito ou alocação de recursos públicos podem perpetuar ou até mesmo amplificar vieses e desigualdades sociais existentes, se forem treinados com dados históricos enviesados [Soares e Aquino 2023]. Isso pode levar a decisões automatizadas que tratam injustamente grupos minoritários ou comunidades vulneráveis, impactando a equidade urbana.

4.1.4. Ataques Cibernéticos: Tipos e Impactos Urbanos

As vulnerabilidades nas plataformas IoT, sistemas de vigilância e infraestruturas de dados criam oportunidades para ataques cibernéticos sofisticados que podem paralisar cidades inteiras [CISA 2023]. Existem três categorias principais de ataques que representam ameaças críticas:

- **Ataques de Negação de Serviço Distribuída (DDoS):** Visam sobrecarregar a rede ou os servidores de serviços essenciais (energia, transporte) com tráfego ilegítimo, causando paralisação e interrupção dos serviços [Cui et al. 2018].
- **Ransomware:** Ataques que sequestram dados ou sistemas inteiros, exigindo um resgate para a restauração. Casos de ransomware em computadores municipais já trouxeram operações urbanas a um estado de paralisação [Cui et al. 2018].
- **Interceptação de Dados:** A comunicação entre dispositivos IoT e a plataforma central pode ser interceptada, permitindo que hackers obtenham dados sensíveis ou injetem comandos maliciosos, comprometendo a integridade e a confidencialidade das informações [Ijaz et al. 2016].

Esses ataques não são meramente técnicos; eles têm implicações diretas para a vida dos cidadãos, afetando desde a mobilidade urbana até a disponibilidade de serviços de saúde e segurança pública. A interconexão massiva de dispositivos e sistemas nas Smart Cities expande a superfície de ataque, tornando a segurança um desafio crítico que requer abordagens integradas e multidimensionais.

4.2. Impactos sobre Direitos Fundamentais e Equidade

Os desafios de segurança, privacidade e ética nas Smart Cities não são apenas questões técnicas; eles representam ameaças concretas aos direitos fundamentais dos cidadãos. A vigilância constante, a coleta massiva de dados e o uso de algoritmos de IA podem impactar profundamente a liberdade individual, a privacidade e a equidade urbana.

4.2.1. Vigilância e Liberdade Individual

A vigilância constante e a capacidade de perfilamento podem levar a um estado de vigilância que impacta diretamente a liberdade individual [Moura e Silva 2019]. O conhecimento de que se está sendo monitorado pode levar à autocensura e à restrição de comportamentos, afetando a liberdade de expressão e de associação. A possibilidade de uso de dados para controle social ou para influenciar decisões políticas e sociais representa uma ameaça à democracia e à autonomia do cidadão [Neto 2023].

O uso de dados e algoritmos de IA para gerenciar e otimizar a vida urbana pode facilmente se converter em ferramentas de controle social [Neto 2023]. A capacidade de monitorar e prever o comportamento dos cidadãos, embora possa ser usada para segurança pública, também pode ser empregada para fins de policiamento preditivo enviesado ou para a repressão de manifestações e dissidências, transformando a cidade em um ambiente de controle excessivo [Bernardi et al. 2020].

4.2.2. Reidentificação de Dados e Privacidade

Mesmo dados que são inicialmente anonimizados podem ser identificados quando correlacionados com outras fontes de informação [Pramanik et al. 2023]. A combinação de dados de tráfego, câmeras de vigilância e registros de consumo pode permitir a criação de perfis detalhados de indivíduos, revelando hábitos, rotinas e informações sensíveis. Esse risco de reidentificação é amplificado pela capacidade de Big Data e IA de processar grandes volumes de dados de forma cruzada, transformando dados "anônimos" em informações pessoais [Daoudagh et al. 2021].

A infraestrutura ubíqua coleta dados de localização, padrões de mobilidade e interações sociais, muitas vezes sem a percepção ou o consentimento explícito e significativo dos cidadãos. O modelo tradicional de consentimento, baseado em termos de serviço longos e complexos, é inadequado para o ambiente pervasivo das Smart Cities, onde o consentimento deveria ser contextual e granular [Hernandez-Ramos et al. 2021]. A falta de transparência sobre quais dados são coletados, como são armazenados e como são utilizados mina a confiança pública e viola princípios fundamentais de proteção de dados.

4.2.3. Exclusão Digital e Desigualdade

As tecnologias de Smart Cities podem exacerbar as desigualdades existentes. A falta de acesso e de familiaridade com as novas tecnologias (exclusão digital) pode criar uma divisão entre os "cidadãos inteligentes" e aqueles que são deixados para trás. A implementação de soluções tecnológicas deve ser guiada por um princípio de equidade, garantindo que os benefícios sejam distribuídos de forma justa e que as tecnologias não criem novas barreiras de acesso a serviços essenciais [JAI 2016].

A discriminação algorítmica é uma preocupação ética central. Algoritmos de IA utilizados em sistemas de segurança, concessão de crédito ou alocação de recursos públicos podem perpetuar ou até mesmo amplificar vieses e desigualdades sociais existentes, se forem treinados com dados históricos enviesados [Soares e Aquino 2023]. Isso pode levar a decisões automatizadas que tratam injustamente grupos minoritários ou comunidades vulneráveis, impactando a equidade urbana e aprofundando as divisões sociais.

4.3. Estratégias de Mitigação: Do Design à Regulação

Para mitigar os desafios identificados, a literatura especializada propõe a adoção de abordagens proativas e regulatórias que integram design ético, arquiteturas técnicas resilientes e marcos regulatórios claros. Essas estratégias devem trabalhar em conjunto para garantir que as Smart Cities sejam desenvolvidas de forma segura, ética e inclusiva.

4.3.1. Design Ético e Seguro desde a Origem

Para mitigar os desafios identificados, a literatura especializada propõe a adoção de abordagens proativas que começam no design dos sistemas:

- **Privacy by Design (PbD):** Incorporação de mecanismos de proteção de dados e privacidade por padrão, e não como um complemento posterior [Ziosi et al. 2022]. Isso significa que, desde a concepção de uma plataforma IoT ou sistema de vigilância, a privacidade deve ser considerada como um requisito fundamental, não uma funcionalidade adicional.
- **Security by Design (SbD):** Desenvolvimento de sistemas com segurança inerente, focando na resiliência contra ataques e na proteção contra vulnerabilidades [König 2021]. Isso aborda diretamente as vulnerabilidades em dispositivos IoT identificadas anteriormente, garantindo que a segurança seja parte integral do desenvolvimento.
- **Transparência e Explicabilidade (XAI):** Garantir que os algoritmos de IA sejam compreensíveis e que as decisões automatizadas possam ser explicadas aos cidadãos [König 2021]. Isso mitiga os riscos de discriminação algorítmica e controle social não transparente, permitindo auditoria e accountability.

4.3.2. Arquiteturas Técnicas Resilientes

Além do design, a adoção de arquiteturas técnicas específicas pode aumentar significativamente a resiliência das Smart Cities:

- **Arquitetura Zero Trust:** Assume que nenhuma entidade é confiável por padrão, exigindo verificação rigorosa para todos os acessos [Cui et al. 2018]. Essa abordagem é particularmente eficaz contra ataques que exploram vulnerabilidades em dispositivos IoT ou tentam interceptar dados entre sistemas, conforme demonstrado na Figura 6. O modelo Zero Trust implementa verificação contínua de identidade, dispositivo, rede e dados.
- **Edge Computing:** A descentralização do processamento de dados pode reduzir a dependência de data centers centrais, diminuindo a latência e o impacto de um ataque em toda a infraestrutura [Khan et al. 2020]. Isso também reduz a quantidade de dados centralizados, mitigando riscos de reidentificação em larga escala e aumentando a privacidade local.
- **Blockchain:** Tecnologias como blockchain são exploradas para criar registros de dados imutáveis e transparentes [Fonseca 2023], oferecendo uma camada adicional de confiança e auditabilidade. A natureza distribuída do blockchain reduz pontos únicos de falha e aumenta a transparência das transações.

4.3.3. Regulação e Políticas Públicas

A intervenção regulatória e a criação de políticas públicas claras são essenciais para equilibrar a inovação tecnológica com a proteção dos direitos fundamentais [Carreño-Dueñas 2016]. A aplicação rigorosa de leis de proteção de dados como a LGPD e a GDPR estabelece um marco legal para o tratamento de dados pessoais [Neto 2023]. Essas legislações definem direitos dos cidadãos, obrigações das organizações e penalidades para violações.

Além disso, a criação de diretrizes específicas para o uso de IA em serviços públicos e a promoção da participação cidadã no desenvolvimento de soluções tec-

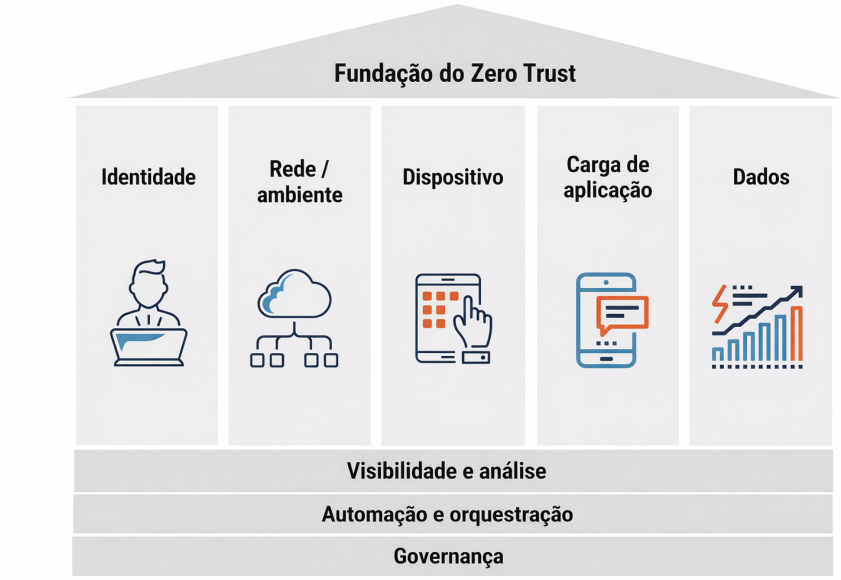

Figura 6. Modelo de segurança Zero Trust, arquitetura que assume que nenhuma entidade é confiável por padrão, exigindo verificação contínua de identidade, dispositivo, rede e dados. Adaptado de HKPR (2024).

nológicas são medidas cruciais para garantir que as Smart Cities sejam desenvolvidas de forma ética, justa e inclusiva [Scott 2019]. A governança participativa, onde cidadãos, governo e setor privado colaboram na definição de políticas, é fundamental para alinhar inovação tecnológica com valores sociais.

4.4. Síntese Integrada: Mapeamento de Desafios e Soluções

A tabela a seguir consolida os principais achados desta análise, articulando os problemas específicos mapeados na literatura com as respectivas propostas de mitigação. A estrutura demonstra como as soluções técnicas, éticas e regulatórias se conectam para endereçar os desafios identificados:

Tabela 3. Síntese Integrada dos Desafios, Implicações e Soluções

Subseção Temática	Principais Desafios e Implicações	Soluções e Mitigações Propostas
Plataformas IoT	Vulnerabilidades em dispositivos IoT, senhas padrão fracas, falta de mecanismos de atualização de firmware.	Implementação de **Security by Design (SbD)** no ciclo de vida dos produtos, gestão rigorosa de patches e criptografia forte.
Sistemas de Vigilância	Coleta massiva de dados sem consentimento claro, tensão entre segurança e privacidade.	Implementação de **Privacy by Design (PbD)**, consentimento contextual e granular, conformidade com LGPD/GDPR.

Continua na próxima página

Tabela 3 – Continuação

Subseção Temática	Principais Desafios e Implicações	Soluções e Mitigações Propostas
Inteligência Artificial	Discriminação algorítmica, vieses em dados de treinamento, falta de transparência.	Auditoria de algoritmos, dados de treinamento imparciais, **Explicabilidade (XAI)** e regulação de IA.
Ataques Cibernéticos	DDoS, Ransomware e Interceptação de Dados podem paralisar serviços essenciais.	Adoção de **arquiteturas Zero Trust** e **Edge Computing** para aumentar resiliência e descentralizar pontos de falha.
Vigilância e Liberdade	Autocensura, restrição de comportamentos, ameaça à democracia e autonomia.	Transparência e Explicabilidade (XAI), participação cidadã, diretrizes éticas e governança participativa.
Reidentificação de Dados	Dados anonimizados podem ser reidentificados através de correlação com múltiplas fontes.	Técnicas robustas de anonimização, descentralização de dados com Edge Computing, regulação rigorosa.
Exclusão Digital	Falta de acesso às tecnologias cria divisão entre cidadãos, amplifica desigualdades.	Políticas de inclusão digital, acesso equitativo a serviços, educação tecnológica e design inclusivo.

5. Considerações Finais

Este trabalho realizou um estudo exploratório sobre a complexa interseção entre a computação ubíqua e o desenvolvimento de cidades inteligentes, com foco nos desafios de segurança, privacidade e ética. A pesquisa sintetizou os principais achados da literatura, que apontam para uma crescente preocupação com a proteção dos cidadãos em ambientes urbanos cada vez mais conectados. Verificou-se que, embora as tecnologias de computação ubíqua, como a Internet das Coisas (IoT) e o Big Data, ofereçam um potencial transformador para a gestão urbana, elas também introduzem vulnerabilidades significativas.

A fragilidade dos dispositivos IoT, a possibilidade de ciberataques a infraestruturas críticas e os riscos associados à coleta e ao processamento massivo de dados pessoais emergem como os principais desafios técnicos a serem enfrentados. A pesquisa destacou também as profundas implicações éticas da vigilância e do perfilamento dos cidadãos, que podem levar à erosão da confiança, à discriminação algorítmica e à perda de autonomia individual.

Em resposta a esses desafios, a literatura aponta para a necessidade de uma abordagem multifacetada. Essa abordagem deve combinar a adoção de princípios de Privacy by Design e Security by Design, o desenvolvimento de arquiteturas de segurança mais robustas e descentralizadas, como o modelo Zero Trust, e a implementação de políticas

públicas e regulamentações claras, a exemplo da Lei Geral de Proteção de Dados (LGPD) no Brasil e do General Data Protection Regulation (GDPR) na Europa.

É importante reconhecer, contudo, as limitações desta pesquisa. Por se tratar de um estudo qualitativo e exploratório, baseado em uma revisão bibliográfica, os resultados aqui apresentados refletem o estado da arte documentado na literatura e não incluem uma análise empírica da implementação das soluções propostas. A pesquisa também se concentrou em quatro domínios específicos: segurança pública, mobilidade urbana, saúde e governança digital. Isso significa que outras áreas de aplicação das cidades inteligentes podem apresentar desafios e soluções distintas que não foram abordadas. Adicionalmente, a rápida evolução tecnológica faz com que novas ameaças e vulnerabilidades surjam constantemente, de modo que a literatura pode não abranger as questões mais recentes e ainda não documentadas.

Diante do exposto, e considerando as lacunas identificadas, recomenda-se que estudos futuros se aprofundem em algumas áreas específicas. Seria de grande valia a realização de pesquisas empíricas, como estudos de caso em cidades que já implementaram soluções de smart cities, para avaliar a eficácia das medidas de segurança e privacidade adotadas e compreender a percepção dos cidadãos sobre essas tecnologias.

No campo técnico, há uma necessidade contínua de desenvolver e testar novos protocolos de segurança para dispositivos IoT, bem como de aprimorar as técnicas de anonimização e proteção de dados. Do ponto de vista ético e social, futuras pesquisas poderiam se dedicar à elaboração e validação de modelos de governança de dados mais participativos, que envolvam os cidadãos na tomada de decisões sobre o uso de suas informações.

Estudos comparativos entre as legislações de diferentes países sobre proteção de dados em cidades inteligentes também poderiam fornecer insights valiosos para o aprimoramento do arcabouço regulatório. Por fim, a realização de estudos longitudinais permitiria analisar os impactos de longo prazo das tecnologias de cidades inteligentes na equidade social, na coesão comunitária e na qualidade de vida urbana, garantindo que o desenvolvimento tecnológico caminhe em harmonia com os valores humanos e democráticos.

Referências

Abadía, J. J. P. et al. (2022). A systematic survey of internet of things frameworks for smart city applications. *Sustainable Cities and Society*, 83:103949.

Al-Turjman, F., Zahmatkesh, H., e Shahroze, R. (2022). An overview of security and privacy in smart cities' iot communications. *Transactions on Emerging Telecommunications Technologies*, 33(3):e3677.

Ali, J., Zafar, M. H., Hewage, C., Hassan, S. R., e Asif, R. (2023). The advents of ubiquitous computing in the development of smart cities—a review on the internet of things (iot). *Electronics*, 12(4):1032.

Araujo, R. B. d. (2003). *Computação Ubíqua: Princípios, Tecnologias e Desafios*. Texto de Minicurso apresentado no XXI Simpósio Brasileiro de Redes de Computadores (SBRC), Natal, RN.

Bernardi, E. et al. (2020). Brazilian scenarios for smart cities deployment from public policies perspectives. In *2020 International Smart Cities Conference (ISC2)*, pages 1–6. IEEE.

Boghossian Torres, T. (2017). O computador para o século 21: Desafios de segurança e privacidade após 25 anos. In *Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*.

Carreño-Dueñas, J. A. (2016). Consentimiento informado en investigación clínica: un proceso dinámico. *Persona y Bioética*, 20(2):232–243.

CISA (2023). Cybersecurity best practices for smart cities. `https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf`.

Cities, C. S. (2025). Recife é a sexta cidade mais inteligente e conectada do brasil. https://portal.connectedsmartcities.com.br/2025/09/23/recife-e-a-sexta-cidade-mais-inteligente-e-conectada-do-brasil/. Ranking Geral CSC 2025 - Recife ocupa a 6ª posição nacional.

Cui, L. et al. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*, 6:46134–46145.

Da Cruz França, M. (2020). Cidades inteligentes: revisão atual sobre o tema e uma proposta de um modelo de referência para implantação de cidades inteligentes. Master's thesis, Universidade Estadual de Campinas.

Daoudagh, S. et al. (2021). Data protection by design in the context of smart cities. *Sensors*, 21(21):7167.

Dialnet (2009). Consentimiento informado e intervenciÓn ... https://dialnet.unirioja.es/descarga/articulo/3117386.pdf.

Fonseca, I. C. (2023). *Cidades Inteligentes e Direito, Governação Digital e Direitos: estudos*.

Gray, D. (2024). Mark weiser and the origins of ubiquitous computing. *Metascience*.

Hamid, B. et al. (2019). Cyber security issues and challenges for smart cities. In *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, pages 1–7.

Hernandez-Ramos, J. L. et al. (2021). Security and privacy in internet of things-enabled smart cities: Challenges and solutions. *IEEE Security & Privacy*, 19(1):12–23.

Ijaz, S. et al. (2016). Smart cities: A survey on security concerns. *International Journal of Advanced Computer Science and Applications*, 7(2):612–625.

InternetLab (2022). Cidades inteligentes e dados pessoais: - lapin. https://lapin.org.br/wp-content/uploads/2022/08/Cidades-Inteligentes-e-Dados-Pessoais-InternetLab-ARTIGO-19-e-LAPIN.pdf.

JAI (2016). Cidades inteligentes: Conceitos, plataformas e desafios. In *Congresso da Sociedade Brasileira de Computação*, pages 1–29. SBC.

Khan, L. U., Yaqoob, I., Tran, N. H., et al. (2020). Edge-computing-enabled smart cities: A comprehensive survey. *IEEE Internet of Things Journal*, 7(10):10200–10232.

König, P. D. (2021). Citizen-centered data governance in the smart city: From ethics to accountability. *Sustainable Cities and Society*, 75:103308.

Leite, L. R. C. (2019). *Internet das Coisas (IoT): vulnerabilidades de segurança e desafios*. PhD thesis, Faculdade de Tecnologia de Americana.

Lopes, B. E. V. (2017). *Computação Ubíqua: limitações e desafios*. PhD thesis, Universidade Federal de Ouro Preto.

Loureiro, A. A. F. e Oliveira, L. B. (2009). Computação ubíqua ciente de contexto: Desafios e tendências. In *Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*.

Mecabô, A. e Gueiros, L. (2023). A revolução silenciosa: a computação ubíqua em nossas vidas. *Revista Online Jovens Cientistas e Tecnólogos de Barreiras*, 1(1).

Mondragon-Barrios, L. (2009). Consentimiento informado: una praxis dialogica para la ... PMC.

Moura, F. e Silva, J. d. A. e. (2019). Smart cities: Definitions, evolution of the concept, and examples of initiatives. In *Industry, Innovation and Infrastructure, Encyclopedia of the UN Sustainable Development Goals*, pages 1–10. Springer Nature Switzerland AG.

Neto, G. O. C. (2023). Lgpd, cidades inteligentes e privacidade. *Scientific Society Journal*, 5(1):83–98.

Parini, F. (2021). O direito à privacidade e à imagem nas cidades inteligentes. *Revista da Faculdade de Direito da FMP*, 16(2):158–178.

Pramanik, S. et al. (2023). An overview of iot privacy and security in smart cities. In *AIP Conference Proceedings*, volume 2523, page 020057.

Rapôso, C. (2025). A evoluÇÃo das tecnologias e dos sistemas de informaÇÃo: Uma anÁlise histÓrica dos Últimos 50 anos. *Revista Tópicos*, 3(24).

Santos, D. d. O. e Freitas, E. B. d. (2016). A internet das coisas e o big data inovando os negócios.

Scielo (2014). ¿hay lugar para el consentimiento informado en los ... https://scielo.isciii.es/pdf/bioetica/n30/original3.pdf.

Scott, E. (2019). The trouble with informed consent in smart cities. https://iapp.org/news/a/the-trouble-with-informed-consent-in-smart-cities.

Soares, C. G. e Aquino, L. S. B. (2023). As cidades inteligentes (smart cities) à luz da lei geral de proteção de dados. *Facit Business and Technology Journal*, 1(46):1–15.

Syed, A. S. et al. (2021). Iot in smart cities: A survey of technologies, practices and challenges. *Smart Cities*, 4(2):24.

Weiser, M. (1991). The computer for the 21st century. *Scientific American*, 265(3):94–104.

Whaiduzzaman, M. et al. (2022). A review of emerging technologies for iot-based smart cities. *Sensors*, 22(23):9271.

Ziosi, M. et al. (2022). Smart cities: reviewing the debate about their ethical implications. *AI & Society*, 38(5):2151–2168.