

IOT E CIDADES INTELIGENTES: AVALIAÇÃO DOS IMPACTOS ÉTICOS DA DISCRIMINAÇÃO RACIAL NOS SISTEMAS DE RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

Jéssica Milena Duarte da Rocha¹
Matheus Henrique Borges de Sousa Moraes²
Eutino Júnior Vieira Sirqueira³

RESUMO

O reconhecimento facial é uma tecnologia cada vez mais adotada em cidades inteligentes, especialmente para fortalecer a segurança pública. No entanto, seu uso levanta sérias preocupações éticas, particularmente em relação à discriminação racial. Pesquisas mostram que esses sistemas são mais vulneráveis a identificar erroneamente indivíduos negros e outras minorias, levando a consequências graves, como prisões injustas e o reforço do racismo. Este estudo busca explorar esses desafios éticos e propor maneiras de garantir aplicações mais justas e inclusivas dessa tecnologia, com base em literatura publicada entre 2014 e 2024, que examina as interseções entre ética, cidades inteligentes e discriminação racial. As análises revelam que o uso de conjuntos de dados diversos, a supervisão humana constante e a implementação de regulamentações específicas são estratégias fundamentais para mitigar vieses algorítmicos e garantir maior equidade. Dessa forma, a colaboração entre governos, empresas e sociedade civil torna-se essencial para o desenvolvimento de tecnologias que priorizem a igualdade, a justiça social e o respeito à dignidade humana.

Palavras-chaves: reconhecimento facial; discriminação racial; cidades inteligentes; ética; segurança pública.

ABSTRACT

Facial recognition is a technology increasingly adopted in smart cities, especially to enhance public security. However, its use raises serious ethical concerns, particularly regarding racial discrimination. Research shows that these systems are more likely to misidentify Black individuals and other minorities, leading to severe consequences such as wrongful arrests and the reinforcement of systemic racism. This study aims to explore these ethical challenges and propose ways to ensure fairer and more inclusive applications of this technology, based on literature published between 2014 and 2024 that examines the intersections of ethics, smart cities, and racial discrimination. The analyses reveal that the use of diverse datasets, continuous human oversight, and the implementation of specific regulations are essential strategies to mitigate algorithmic bias and promote greater equity. Therefore, collaboration between governments, companies, and civil society is crucial for the development of technologies that prioritize equality, social justice, and respect for human dignity.

Keywords: facial recognition; racial discrimination; smart cities; ethics; public safety.

¹ Graduanda em Análise e Desenvolvimento de Sistemas. Instituto Federal De Educação, Ciência e Tecnologia do Piauí. jessicamilena118@gmail.com.

² Prof. Esp. Matheus Henrique Borges de Sousa Moraes. Instituto Federal De Educação, Ciência e Tecnologia do Piauí. matheus.morais@ifpi.edu.br.

³ Prof. Esp. Eutino Júnior Vieira Sirqueira. Instituto Federal De Educação, Ciência e Tecnologia do Piauí. eutinojunior@gmail.com.

1 INTRODUÇÃO

O crescimento acelerado das cidades e o aumento da criminalidade geram desafios crescentes para a segurança urbana. Estima-se que mais de 55% da população mundial viva em áreas urbanas, com projeção de alcançar 68% até 2050 (ONU-Habitat, 2022). Esse processo intensifica a necessidade de soluções inovadoras para gestão e segurança nos centros urbanos. Nesse contexto, cidades inteligentes surgem como uma abordagem promissora para enfrentar esses desafios, empregando tecnologias avançadas para melhorar a qualidade de vida e garantir maior segurança para os cidadãos.

Entre as tecnologias aplicadas nas cidades inteligentes, a Internet das Coisas (IoT, do inglês *Internet of Things*) desempenha papel central. Essa tecnologia conecta dispositivos em redes integradas, possibilitando a coleta e o compartilhamento de dados para otimizar a gestão urbana (Gubbi et al., 2013). Um exemplo relevante de tecnologia utilizada na internet das coisas e cidades inteligentes é o reconhecimento facial, que utiliza algoritmos avançados para identificar indivíduos com base em características físicas. Esse recurso tem sido amplamente empregado para apoiar investigações criminais e a segurança pública (Jain, Ross e Nandakumar, 2011; Zhao et al., 2003).

Entretanto, o uso do reconhecimento facial levanta preocupações éticas, sobretudo devido às visões raciais incorporadas nesses sistemas. Estudos apontam que as taxas de erro são significativamente mais altas para pessoas negras e de outras minorias raciais, enquanto pessoas brancas são menos afetadas. Segundo o estudo Reconhecimento facial e a autenticidade: uma questão de vieses étnicos (SBC, 2024), as taxas de erro variam de 1% para pessoas brancas a até 35% para pessoas negras. Essas taxas de erro resultaram, em grande parte, de dados de treinamento racialmente desequilibrados, além de fatores como condições específicas de iluminação e ângulos desfavoráveis das câmeras.

Essas falhas não apenas comprometem a eficácia dos sistemas, mas também reforça o racismo existente, levantando questões éticas sobre o uso de tecnologias que podem perpetuar discriminações estruturais. Diante disso, é essencial compreender e abordar os impactos éticos associados ao reconhecimento facial, garantindo que sua aplicação seja justa e contribua para a equidade social.

A escolha deste tema partiu do interesse em compreender como tecnologias modernas, como o reconhecimento facial, estão sendo incorporadas às cidades inteligentes sem o devido cuidado ético. Ao investigar mais profundamente, percebeu-se que essas ferramentas, que deveriam promover segurança e inovação, muitas vezes acabam reforçando desigualdades, principalmente raciais. A motivação veio do desejo de entender como essas tecnologias podem afetar negativamente pessoas negras e grupos vulneráveis, e também de contribuir com uma reflexão crítica sobre o uso da tecnologia no espaço público. Trata-se de um tema atual, necessário e diretamente ligado a debates sobre direitos humanos, justiça social e inovação.

Este estudo busca compreender os impactos éticos da discriminação racial em sistemas de reconhecimento facial nas cidades inteligentes. A pesquisa é guiada por três pilares principais:

Impactos Éticos: Explorar os dilemas e desafios que surgem quando essas tecnologias reforçam preconceitos raciais.

Estudos de Caso: Examinar situações reais para entender como esses problemas se manifestam na prática.

Soluções e Mitigação: Pensar em formas concretas de reduzir esses vieses e garantir que o uso dessas ferramentas seja mais justo e responsável.

Além disso, o estudo procura responder a três questões fundamentais:

1. Quais são os desafios éticos do uso de reconhecimento facial na segurança pública?
2. De que forma a falta de diversidade nos dados de treinamento afeta a precisão e a confiabilidade dos sistemas de reconhecimento facial?
3. Quais medidas e regulamentações podem reduzir os riscos do reconhecimento facial?

Com essa abordagem, o estudo espera não apenas contribuir com o debate acadêmico, mas também inspirar mudanças práticas que tornem as cidades mais inclusivas e acolhedoras, onde a tecnologia sirva como aliada na promoção da igualdade e justiça social.

2. METODOLOGIA

Esta pesquisa foi conduzida com o objetivo de compreender os impactos éticos da discriminação racial em sistemas de reconhecimento facial no contexto de cidades inteligentes. Para isso, adotamos uma abordagem qualitativa e exploratória, baseada na revisão de literatura. Esse caminho foi escolhido porque permite explorar com profundidade os dilemas éticos associados a essas tecnologias, além de identificar lacunas e estimular reflexões importantes sobre o tema.

Os dados utilizados foram coletados a partir de artigos acadêmicos, livros, teses, documentos oficiais e relatórios técnicos. As principais bases de pesquisa incluíram Scielo, IEEE Xplore e Google Scholar, onde buscamos por materiais relacionados a “reconhecimento facial”, “discriminação racial”, “cidades inteligentes”, “ética tecnológica” e “IoT”. Para garantir a relevância e atualidade das informações, priorizamos publicações dos últimos nove anos (2014-2024), focando em estudos que discutissem os aspectos éticos e os impactos na segurança pública. Materiais que não se conectavam diretamente a essas questões foram descartados.

O processo de análise envolveu a identificação de temas centrais, como os principais desafios éticos, os efeitos da discriminação racial e as possíveis soluções para tornar essas tecnologias mais justas e inclusivas. Essa organização foi guiada por três pilares fundamentais: os impactos éticos, estudos de caso concretos e estratégias de mitigação para os problemas encontrados.

É importante destacar que esta pesquisa apresenta algumas limitações. Por depender exclusivamente de fontes secundárias, carecemos de experimentações práticas ou análises quantitativas. Além disso, identificamos uma possível escassez de estudos específicos sobre o tema no contexto brasileiro, o que sugere a necessidade de novos trabalhos na área.

Tabela da Metodologia

Etapa	Descrição
Fontes de Dados	Artigos acadêmicos, livros, teses, documentos oficiais e relatórios técnicos.
Bases de Pesquisa	Scielo, IEEE Xplore, Google

Fonte: Elaboração própria.

3 REFERENCIAL TEÓRICO

3.1. CIDADES INTELIGENTES

Conforme a Carta Brasileira para Cidades Inteligentes (Brasil, 2020), as cidades inteligentes são aquelas comprometidas com o desenvolvimento urbano e a transformação digital sustentável, nos aspectos econômicos, ambientais e socioculturais. Essas cidades atuam de forma planejada, inovadora, inclusiva e em rede, promovendo a governança e a gestão colaborativa. Além disso, utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir a desigualdade, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas. Também é garantido o uso seguro e responsável de dados e das tecnologias da informação e comunicação (Brasil, 2020).

O conceito de cidade inteligente abrange muitas dimensões, buscando equilibrar a inovação tecnológica com inclusão social, governança participativa e redução do impacto ambiental. Segundo Giffinger et al. (2007), uma cidade inteligente deve ser competitiva e inovadora, incentivando o empreendedorismo, a produtividade e a flexibilidade no mercado de trabalho, além de promover a inserção internacional. Ela também deve investir no capital humano, favorecendo o nível de qualificação, criatividade e participação ativa dos cidadãos na vida pública, garantindo a diversidade étnica e social. A participação da população na tomada de decisões e a transparência na gestão pública são fundamentais, assim como a eficiência dos serviços públicos.

Além disso, uma cidade inteligente deve contar com uma infraestrutura de transporte acessível e sustentável, promovendo a mobilidade tanto local quanto internacional, apoiada por tecnologias de informação e comunicação (TICs). A gestão dos recursos naturais e a promoção da eficiência energética são outras áreas essenciais, com políticas voltadas para a sustentabilidade e o uso responsável dos recursos. Por fim, a qualidade de vida na cidade inteligente é assegurada por serviços essenciais de saúde, segurança, educação, cultura e lazer, que são acessíveis e de alta qualidade para todos os cidadãos.

Giffinger et al. (2007) ressaltam que a adoção de iniciativas que integrem essas dimensões é crucial para a transformação de um espaço urbano em uma cidade inteligente. A aplicação de tecnologias emergentes, como IoT, *Big Data* e inteligência artificial, é fundamental para oferecer soluções inovadoras e eficazes para os desafios urbanos.

Segundo Komninos (2018), o conceito de cidades inteligentes vai além da simples incorporação de tecnologias avançadas. O autor explica que essas cidades desenvolvem capacidades locais de inovação, fortalecendo o papel das comunidades no processo de transformação digital, o que contribui para um ambiente de governança colaborativa e inclusão social.

Para exemplificar, cidades como Barcelona, Cingapura e Curitiba adotam estratégias inteligentes em áreas como mobilidade urbana, eficiência energética e inclusão social. Barcelona, por exemplo, implementou sensores inteligentes em seu sistema de gestão hídrica, reduzindo em 25% as perdas de água. Já Cingapura investe amplamente em inteligência artificial para otimizar o transporte público e a sincronização de semáforos, reduzindo o tempo de deslocamento. Curitiba, por sua vez, aplica inteligência artificial na gestão do transporte público, melhorando a eficiência e reduzindo a pegada de carbono (Nautilus Sustentável, 2024; Caos Planejado, 2024; Levisky, 2023).

Essa abordagem integrada, em conformidade com a Carta Brasileira para Cidades Inteligentes (Brasil, 2020), busca não apenas atender às necessidades urbanas imediatas, mas também promover um desenvolvimento urbano sustentável, inclusivo e resiliente a longo prazo e com segurança. O uso do reconhecimento facial em cidades inteligentes surge como uma ferramenta estratégica que aprimora diversos aspectos da gestão urbana, principalmente no que se refere à segurança pública, mobilidade urbana e personalização de serviços.

A tecnologia do reconhecimento facial oferece a capacidade de identificar indivíduos em tempo real, monitorar fluxos populacionais e controlar o acesso a espaços públicos e privados, permitindo uma gestão mais eficiente e ágil. Por exemplo, o reconhecimento facial pode ser utilizado em sistemas de monitoramento de tráfego para agilizar o fluxo de veículos ou em áreas de segurança para detectar comportamentos suspeitos (Jusbrasil, 2023).

Além disso, essa tecnologia é valiosa para melhorar a experiência do cidadão, ao permitir a personalização de serviços como o atendimento em espaços públicos, transportes e sistemas de pagamento, adaptando-se às necessidades de cada usuário de forma mais eficiente. Dessa forma, as cidades inteligentes podem promover uma maior conveniência, segurança e conforto para seus habitantes (NEC, 2023).

Entretanto, a implementação do reconhecimento facial envolve desafios significativos, principalmente no que diz respeito a questões éticas. A proteção da privacidade dos cidadãos deve ser priorizada, garantindo que o uso de dados pessoais esteja em conformidade com as regulamentações e leis de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados) (Planalto, 2018).

Ainda conforme a Lei Geral de Proteção de Dados (LGPD), é essencial obter o consentimento explícito das pessoas para o uso de suas imagens, o que pode ser um desafio em ambientes urbanos amplos (Planalto, 2018). Além disso, a mitigação de vieses algorítmicos é crucial, uma vez que sistemas de reconhecimento facial podem apresentar falhas na identificação de pessoas de diferentes etnias, o que pode gerar discriminação ou injustiças no tratamento de indivíduos (IBM, 2024).

Assim, embora o reconhecimento facial apresente uma série de benefícios em termos de segurança e eficiência, sua adoção deve ser cuidadosamente planejada e regulamentada, a fim de minimizar os riscos associados à sua implementação.

3.2. RECONHECIMENTO FACIAL

O reconhecimento facial é uma tecnologia biométrica que identifica indivíduos por meio da análise de características faciais únicas, utilizando algoritmos avançados para processar imagens. Recentemente, a autenticação facial em 3D tem ganhado destaque, pois captura detalhes tridimensionais do rosto, como contornos e texturas, oferecendo maior precisão e dificultando fraudes (Gryfo, 2025). Além disso, o reconhecimento facial em tempo real tem se tornado viável devido a avanços em algoritmos e processamento, permitindo aplicações em grandes eventos e transporte público (Connected Smart Cities, 2024).

Nas cidades inteligentes, o reconhecimento facial tem sido implementado para aprimorar a segurança pública e otimizar serviços urbanos. Governos utilizam essa tecnologia em sistemas de videomonitoramento para identificar e prevenir delitos, localizar suspeitos e monitorar eventos públicos. Por exemplo, Curitiba adotou a "Muralha Digital", um sistema de videomonitoramento que utiliza inteligência artificial para tornar mais eficientes suas cerca de 1.600 câmeras fixas, agora equipadas com reconhecimento facial capaz de identificar indivíduos com base em características faciais únicas e comparar essas informações com bancos de dados de pessoas procuradas (Prefeitura Municipal de Curitiba, 2025).

As técnicas atuais de reconhecimento facial são baseadas em inteligência artificial, aplicando aprendizado de máquina e redes neurais profundas. Modelos modernos são treinados com grandes bases de dados compostas por milhões de imagens, processadas por arquiteturas avançadas como Vision Transformers (ViTs) e ResNet (He et al., 2016), que melhoram a capacidade de generalização e extração de padrões visuais robustos. Além disso, técnicas como aprendizado contrastivo e perda tripla (Schroff et al., 2015) ajudam a aprimorar a precisão da identificação ao otimizar o espaço de representação facial.

A diversidade e a qualidade dos dados utilizados no treinamento desses modelos são fundamentais para seu desempenho. Bases de dados que incluem rostos de diferentes etnias, idades, gêneros e condições de iluminação garantem que os modelos sejam mais justos e eficazes em cenários reais. A falta de diversidade pode levar a vieses algorítmicos, resultando em identificações imprecisas, especialmente para grupos sub-representados (Gryfo, 2025). Assim, garantir a inclusão de um conjunto amplo e equilibrado de dados durante o treinamento é essencial para a confiabilidade e segurança das aplicações de reconhecimento facial.

No entanto, o uso crescente do reconhecimento facial levanta preocupações sobre privacidade e proteção de dados. Regulamentações recentes enfatizam que os indivíduos não devem ser obrigados a utilizar o reconhecimento facial para verificação de identidade, destacando a importância de oferecer alternativas e obter consentimento explícito antes de processar dados faciais (Planalto, 2018). Portanto, é crucial que o desenvolvimento e a implementação dessas tecnologias sejam acompanhados por políticas que garantam a transparência e o respeito aos direitos individuais.

3.3. CIDADES INTELIGENTES E O USO DO RECONHECIMENTO FACIAL

O conceito de cidades inteligentes surge como uma resposta inovadora aos desafios urbanos contemporâneos, como segurança pública, mobilidade e sustentabilidade. As cidades inteligentes fazem uso de tecnologias avançadas, como dispositivos conectados por meio da IoT, para melhorar a qualidade de vida dos cidadãos. O reconhecimento facial, uma dessas tecnologias, tem sido amplamente implementado em iniciativas de segurança pública, permitindo a identificação de indivíduos com base em suas características faciais por meio de algoritmos sofisticados.

Entretanto, apesar de seu potencial, o uso do reconhecimento facial levanta questões éticas significativas. A principal preocupação envolve os vieses raciais, que podem afetar negativamente grupos marginalizados, especialmente as minorias raciais. Um estudo realizado pelo Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos, em 2020, revelou que os sistemas de reconhecimento facial apresentaram taxas de erro mais altas para indivíduos negros e de outras etnias em comparação com pessoas brancas. Esse resultado evidencia como os preconceitos presentes na sociedade acabam sendo transmitidos para a tecnologia, reforçando problemas que deveriam ser superados (NIST, 2020).

O documentário *Coded Bias* (2020), de Joy Buolamwini, revela como os sistemas de reconhecimento facial e outras tecnologias de inteligência artificial podem amplificar preconceitos raciais e de gênero. O estudo mostra que as taxas de erro são significativamente mais altas para mulheres negras, evidenciando a falta de diversidade e representatividade nas bases de dados usadas para treinar esses sistemas. Isso demonstra como a tecnologia, muitas vezes, reproduz e intensifica desigualdades raciais preexistentes, levantando questões sobre a necessidade de maior inclusão e diversidade no desenvolvimento dessas ferramentas. O *Coded Bias* chama a atenção para as implicações éticas e sociais dessas falhas, especialmente quando aplicado em áreas sensíveis como segurança pública, (Buolamwini, 2020).

4. IMPACTOS ÉTICOS

Esta seção aborda os impactos éticos do reconhecimento facial, destacando os problemas raciais gerados pela falta de representatividade nos dados de treinamento. Serão discutidos os efeitos dessas falhas, como erros de identificação e reforço de estereótipos raciais, além das implicações para direitos humanos e justiça social.

4.1 PROBLEMAS RACIAIS EM SISTEMAS DE RECONHECIMENTO FACIAL

Os problemas raciais nos sistemas de reconhecimento facial surgem principalmente devido à falta de representatividade nas bases de dados utilizadas para treinar os algoritmos. Muitas dessas bases contêm predominantemente imagens de pessoas brancas, o que diminui a precisão dos sistemas na identificação de indivíduos de outras etnias. O estudo *Gender Shades* de Buolamwini e Gebru (2018) é um exemplo claro dessa disparidade: ele mostrou que sistemas de reconhecimento facial de empresas de tecnologia apresentaram taxas de erro superiores a 35% para mulheres negras, enquanto para homens brancos a taxa de erro foi inferior a 1%. Os sistemas de reconhecimento facial, ao refletirem preconceitos, podem prejudicar ainda mais as pessoas que já enfrentam maiores desafios (Buolamwini & Gebru, 2018).

Além disso, fatores tecnológicos, como iluminação envolvente e ângulos desfavoráveis das câmeras, podem agravar os erros, especialmente para indivíduos com pele mais escura. Estudos indicam que tais falhas tecnológicas estão voltadas para a exclusão de grupos marginalizados, com consequências graves, como prisões injustas e perpetuação de estereótipos raciais (Krishnapriya et al., 2020). Esses problemas também foram documentados em análises sobre o uso de reconhecimento facial por forças policiais, que destacam o impacto desproporcional dessas tecnologias em comunidades marginalizadas, gerando riscos como discriminação e visibilidade de direitos civis (Garvie et al., 2016).

4.2. AS IMPLICAÇÕES ÉTICAS DO RECONHECIMENTO FACIAL

O uso de sistemas de reconhecimento facial, especialmente em cidades inteligentes, pode promover a discriminação racial, principalmente quando os dados utilizados para treiná-los são desequilibrados. Isso cria um ciclo em que as minorias são constantemente prejudicadas, aumentando o risco de erros de identificação, como prisões indevidas, afetando principalmente pessoas negras e outros grupos marginalizados. Além disso, há um risco crescente de que esses sistemas reforcem estereótipos contratados, associando-se de forma injusta a indivíduos de determinadas raças à criminalidade, criando uma falsa percepção de que toda pessoa negra é potencialmente criminoso (Brasil de Fato, 2022).

Essas questões não são apenas técnicas, mas têm implicações diretas em direitos humanos e justiça social. Quando uma tecnologia falha, ela pode minar a confiança pública nas autoridades, além de violar direitos fundamentais, como o direito à privacidade. O uso envolvido de vigilância em comunidades vulneráveis também pode gerar um clima de desconfiança e medo, especialmente quando essas tecnologias são aplicadas de maneira desigual, reforçando ainda mais o racismo e criando ainda mais conflitos sociais e reforçando barreiras entre as pessoas (G1 Globo, 2023).

5. ESTUDOS DE CASO

Esta seção apresenta casos reais de falhas em sistemas de reconhecimento facial, destacando erros de identificação, discriminação racial e consequências negativas em áreas como segurança pública e serviços. Os exemplos ressaltam a necessidade de mais regulamentação, supervisão e melhorias tecnológicas para proteger os direitos dos cidadãos.

5.1. CASOS PRÁTICOS E EVIDÊNCIAS REAIS

Os sistemas de reconhecimento facial têm sido alvo de críticas intensas devido às falhas e aos impactos negativos que podem causar. Um dos casos mais emblemáticos foi o do ator Michael B. Jordan, que, apesar de ser uma figura pública extremamente confiável, foi erroneamente identificado como suspeito em uma investigação. Esse erro revelou que a tecnologia pode falhar até mesmo com pessoas de alta visibilidade, gerando constrangimento e destacando os perigos de confiança exclusivamente em sistemas automatizados em situações críticas, como investigações criminais. O caso impulsionou debates sobre a necessidade de supervisão humana para evitar equívocos e proteger os direitos dos cidadãos (O Dia, 2022).

Outro episódio marcante envolveu Robert Williams, um homem negro preso injustamente em Detroit após ser identificado de forma incorreta por um sistema de reconhecimento facial utilizado pela polícia. A falha no sistema levou à sua prisão sem justificativa válida, causando transtornos pessoais, profissionais e emocionais. Esse é um exemplo onde sistemas de reconhecimento facial podem apresentar maior probabilidade de erro ao lidar com pessoas racializadas. Esse caso gerou debates amplos sobre regulamentação, supervisão humana e a necessidade de revisões nos algoritmos para evitar discriminação (Time, 2022).

Uma investigação realizada em 2023 revelou o uso desproporcional da tecnologia de reconhecimento facial pela polícia de Nova Orleans, que se aplicava com maior frequência em áreas predominantemente negras. Essa prática não apenas reforçou desigualdades históricas, mas também gerou insegurança em comunidades já marginalizadas, ampliando a percepção de injustiça no sistema de vigilância. O caso foi apontado como um exemplo claro de como essas ferramentas podem ser empregadas de maneira discriminatória, aprofundando disparidades raciais (SciELO, 2023).

Em 2024, a Clearview AI, uma das empresas mais criticadas no setor de reconhecimento facial, esteve no centro de novos relatos de prisões injustas. Um dos casos mais graves foi o de uma pessoa negra erroneamente identificada como suspeita de um crime. A repercussão reacendeu debates sobre a ausência de regras dessas ferramentas, levantando questionamentos sobre a precisão de seus algoritmos e os riscos de vieses raciais, além de destacar a importância de maior transparência e supervisão no uso dessas tecnologias em contextos legais e policiais (The Verge, 2024).

No campo da tecnologia de consumo, estudos realizados em 2024 destacaram falhas nos sistemas de desbloqueio facial de smartphones. Essas ferramentas foram prejudicadas significativamente em consideração às pessoas racializadas, com um impacto especialmente severo para mulheres negras. Usuários relatando transtornos ao tentar acessar seus dispositivos, evidenciando a falta de diversidade no treinamento de algoritmos. Esses problemas levantaram questionamentos sobre a responsabilidade das empresas em desenvolver soluções mais inclusivas e representativas de toda a população (G1.Globo, 2024).

No Brasil, em março de 2024, os irmãos gêmeos enfrentaram dificuldades ao utilizar sistemas de reconhecimento facial em aplicativos bancários e no portal gov.br. Os sistemas incapazes de diferenciar entre os dois impedem o acesso a serviços essenciais, como movimentações financeiras e consultas governamentais. O episódio destacou as limitações técnicas dessas tecnologias em lidar com características físicas semelhantes e reforçou a necessidade de aprimorar os algoritmos para evitar transtornos a usuários legítimos (Acessa.Com, 2024).

Ainda em 2024, um turista em Brasília conseguiu enganar um sistema de reconhecimento facial, abrindo a porta de um prédio na W3 Norte sem nunca ter estado no local anteriormente. O incidente levantou questionamentos sobre a confiabilidade desses sistemas como medida de segurança em residências. A vulnerabilidade demonstrada reforçou a necessidade de implementar medidas adicionais, como autenticações complementares, para garantir maior eficácia e proteção (G1.Globo, 2024).

Outro caso ocorreu durante uma conferência no Rio de Janeiro, em que uma psicóloga foi impedida de acessar o evento devido a um erro em um sistema de reconhecimento facial. O caso gerou constrangimento em um ambiente profissional, prejudicando a audiência do incidente e levantando críticas à aplicação dessas tecnologias em eventos sociais e corporativos. Esse caso evidencia o impacto de erros que podem comprometer a confiança, a dignidade e o desempenho profissional dos indivíduos (Defensoria Rj, 2024).

Esses episódios ilustram que, embora o reconhecimento facial tenha potencial para trazer benefícios, suas falhas podem resultar em consequências graves. Eles reforçam a necessidade urgente de maior regulamentação, supervisão humana e desenvolvimento de algoritmos mais precisos e éticos, capazes de reduzir vieses e garantir a proteção dos direitos fundamentais.

6. SOLUÇÕES E MITIGAÇÃO

Esta seção aborda soluções para os problemas éticos do reconhecimento facial, incluindo o contexto jurídico e regulamentar em diferentes países. Também discutimos exemplos de sucesso e falhas no uso da tecnologia, além de orientar caminhos para torná-la mais inclusiva e ética, como garantir diversidade nos dados, transparência nos algoritmos e políticas públicas que protegem os direitos individuais.

6.1. CONTEXTUALIZAÇÃO JURÍDICA E REGULATÓRIA

O uso de sistemas de reconhecimento facial em cidades inteligentes envolve diversas questões jurídicas e regulatórias, que têm sido debatidas em diferentes regiões. No Brasil, a LGPD, instituída pela Lei nº 13.709/2018 (Planalto, 2018), regula a coleta e o uso de dados pessoais, incluindo dados biométricos, como os utilizados no reconhecimento facial. Embora a LGPD tenha o objetivo de proteger a privacidade dos cidadãos, a implementação da lei enfrenta desafios, principalmente na aplicação e no cumprimento eficaz quando se trata de tecnologias como o reconhecimento facial.

Na Europa, o Regulamento Geral de Proteção de Dados (GDPR), formalizado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (União Europeia, 2016), estabelece regras rigorosas sobre a proteção da privacidade e o uso de dados pessoais. O GDPR entrou em vigor em 25 de maio de 2018 e define diretrizes para a coleta, processamento, armazenamento e compartilhamento de dados, garantindo a segurança e a privacidade dos cidadãos europeus. Ele se baseia em princípios fundamentais, como licitude, lealdade e transparência no tratamento dos dados, minimização da coleta, limitação de armazenamento, exatidão, integridade e responsabilidade.

O regulamento também confere aos titulares de dados direitos importantes, como o direito de acesso, retificação, esquecimento, portabilidade, objeção e restrição do processamento. Em relação ao reconhecimento facial, o GDPR classifica os dados biométricos como categoria especial e impõe restrições rigorosas ao seu uso, exigindo consentimento explícito ou justificativa legal adequada.

Nos Estados Unidos, a regulamentação varia de estado para estado. Algumas cidades, como São Francisco, proibiram o uso do reconhecimento facial em espaços públicos devido a preocupações com a privacidade e as visões raciais (Stolberg, 2019). Em contraste, na China, a tecnologia de reconhecimento facial é amplamente utilizada, gerando preocupações internacionais sobre a vigilância em massa e a violação de direitos humanos (Vigilância Dos Direitos Humanos, 2019).

Em 2024, a Comissão dos Direitos Civis dos EUA destacou a falta de uma legislação federal clara sobre o uso do reconhecimento facial, conforme relatório oficial publicado no mesmo ano (Estados Unidos, 2024). Esse vazio regulatório levanta questões sobre a responsabilidade e os riscos de discriminação, especialmente no que diz respeito às visões raciais em sistemas de vigilância e policiamento.

Além disso, um estudo recente das Academias Nacionais de Ciências, Engenharia e Medicina enfatizou a necessidade de estabelecer padrões equitativos para o uso dessa tecnologia, alertando para a transparência em relação à privacidade e à discriminação racial, especialmente nas populações vulneráveis (Academias Nacionais, 2024).

6.2. CASOS DE SUCESSO E FALHAS NO BRASIL E NO MUNDO

No Brasil, o uso de reconhecimento facial tem sido adotado em grandes eventos públicos e em investigações criminais. Por exemplo, a tecnologia foi

implementada em eventos como o Carnaval do Rio de Janeiro para identificar foragidos nas festas e melhorar a segurança (CNN Brasil, 2024). No entanto, também surgiram preocupações sobre o uso excessivo de tecnologias de vigilância, especialmente em contextos de monitoramento urbano, sem a devida regulamentação.

Em contraste, cidades como São Francisco, nos Estados Unidos, baniram o uso de reconhecimento facial em espaços públicos devido a preocupações com a privacidade e a discriminação racial. Essa decisão tem sido vista como um exemplo positivo de como as autoridades podem priorizar os direitos civis sobre a implementação de tecnologias de vigilância. A restrição do uso de reconhecimento facial tem gerado discussões sobre os impactos dessa decisão, com defensores argumentando que é um passo importante para proteger as liberdades individuais, enquanto opositores apontam que a medida pode comprometer a segurança pública (G1 Globo, 2019).

6.3. CAMINHOS PARA UMA TECNOLOGIA MAIS INCLUSIVA

Fazer com que o reconhecimento facial seja mais justo e ético vai muito além de ajustes técnicos. Trata-se de uma questão de respeito pela diversidade e pelos direitos de cada pessoa. Para que essa tecnologia se torne verdadeiramente benéfica para a sociedade, é fundamental adotar práticas que coloquem as pessoas, suas necessidades e direitos, no centro de todas as decisões.

Um ponto crucial é garantir que os bancos de dados usados para treinar os sistemas de reconhecimento facial representem a diversidade humana presente no mundo real. Isso significa incluir imagens de pessoas de diferentes etnias, gêneros, idades e origens sociais, o que contribui para a redução de erros que afetam de forma desproporcional grupos marginalizados. Afinal, todos têm o direito de serem reconhecidos com igualdade e respeito.

Além disso, a transparência dos algoritmos é essencial para construir a confiança das pessoas na tecnologia. Os algoritmos devem ser desenvolvidos de maneira clara, permitindo que especialistas externos identifiquem e corrijam eventuais falhas ou preconceitos. Isso inclui a publicação de estudos que expliquem como os algoritmos funcionam, destacando suas limitações e possíveis problemas, bem como a disponibilização de dados anonimizados para auditorias externas seguras.

A criação de processos contínuos de revisão é indispensável para garantir a identificação e correção de preconceitos. Também é fundamental que os desenvolvedores expliquem, de maneira simples e acessível, como as decisões desses sistemas são tomadas, evitando mal-entendidos e promovendo o uso responsável da tecnologia.

As políticas públicas desempenham um papel importante ao proteger os direitos das pessoas. É necessário estabelecer regras claras e éticas que limitem o uso do reconhecimento facial a situações em que ele seja realmente necessário, garantindo que sua aplicação preserve a dignidade humana e evite a ampliação dos preconceitos. Além disso, o diálogo sobre os impactos do reconhecimento facial deve ser ampliado.

O futuro da tecnologia não pode ser decidido por poucas pessoas em reuniões fechadas. É essencial que governos, empresas, pesquisadores e a sociedade participem dessas discussões. Organizar debates e consultas públicas para ouvir diferentes perspectivas, bem como formar reuniões conjuntas com representantes de comunidades, pesquisadores e ativistas, pode contribuir para um entendimento mais amplo sobre os benefícios e os riscos dessa tecnologia. Quanto mais pessoas se envolverem nessas conversas, maior será a chance de usar o reconhecimento facial de forma consciente e respeitosa.

Por fim, as organizações que utilizam essa tecnologia precisam refletir sobre o impacto de suas decisões. Cada dado coletado representa uma pessoa com direitos, e é indispensável adotar práticas éticas que garantam o uso responsável do reconhecimento facial, sempre dentro dos limites legais e morais. Acima de tudo, a tecnologia deve servir às pessoas, e não o contrário. Quando empatia e justiça são colocadas no centro do desenvolvimento tecnológico, o reconhecimento facial pode se tornar uma ferramenta de inclusão, promovendo valores que respeitam os direitos, a dignidade e a diversidade de todos.

7. RESULTADOS E DISCUSSÕES

Os resultados desta pesquisa evidenciaram que o uso de sistemas de reconhecimento facial em segurança pública apresenta desafios significativos, especialmente relacionados à discriminação racial. Estudos demonstraram que indivíduos negros e de outras minorias raciais enfrentam taxas de erro até 35 vezes maiores em comparação a indivíduos brancos. Esses erros têm consequências graves, como prisões injustas, ilustradas por casos práticos, como o de Robert Williams.

Um dos principais fatores que contribuem para esses erros é a falta de diversidade nas bases de dados utilizadas para treinar os algoritmos. Quando essas bases são compostas predominantemente por imagens de pessoas brancas, os sistemas acabam sendo menos precisos ao identificar pessoas de outras etnias, perpetuando preconceitos.

Além dos problemas técnicos, há impactos sociais e jurídicos significativos. O uso desproporcional desses sistemas por forças policiais em comunidades negras agrava o preconceito e pode violar direitos fundamentais, como o direito à privacidade. Esses problemas não apenas prejudicam diretamente as pessoas afetadas, mas também minam a confiança pública nas autoridades, ampliando tensões sociais.

Diante desses desafios, é crucial discutir o papel da tecnologia em cidades inteligentes. Embora o reconhecimento facial tenha o potencial de melhorar a segurança pública, sua aplicação indevida e tecnicamente falha pode perpetuar injustiças. Para evitar isso, é essencial que os desenvolvedores garantam maior representatividade nos dados de treinamento, além de implementar mecanismos de supervisão humana e regulamentações específicas.

Casos práticos, como o de Robert Williams, e falhas em sistemas de desbloqueio facial demonstram a urgência de aprimorar essas tecnologias. Em algumas regiões, como São Francisco, o uso do reconhecimento facial em espaços públicos foi proibido, destacando a importância de estabelecer limites éticos claros para evitar abusos.

No Brasil, a LGPD e, na Europa, o GDPR representam avanços regulatórios importantes. No entanto, ainda é necessário que essas leis sejam aplicadas de forma mais rigorosa no contexto de tecnologias biométricas. É fundamental desenvolver diretrizes específicas que estejam alinhadas a padrões globais de equidade e transparência.

Esses resultados reforçam a necessidade de um debate amplo e colaborativo, envolvendo pesquisadores, desenvolvedores, legisladores e a sociedade civil. Apenas por meio de esforços conjuntos será possível encontrar soluções que equilibrem segurança, inclusão e direitos humanos, promovendo uma implementação ética e responsável dessas tecnologias em cidades inteligentes.

8 CONSIDERAÇÕES FINAIS

As considerações finais deste trabalho destacam a importância de refletir criticamente sobre o uso de tecnologias como o reconhecimento facial, especialmente no contexto da segurança pública em cidades inteligentes. Embora essa tecnologia tenha potencial para contribuir com a identificação de indivíduos e a redução de crimes, os desafios éticos associados, como a discriminação racial, demandam atenção especial.

Os resultados apontaram que os vieses raciais presentes nos algoritmos podem perpetuar desigualdades estruturais, resultando em impactos negativos profundos, como prisões injustas e marginalização de comunidades vulneráveis. Esses problemas ressaltam a necessidade de tornar os sistemas mais justos e inclusivos, garantindo que sua aplicação respeite os direitos humanos e promova a igualdade.

Além disso, a falta de regulamentação específica sobre o uso dessas tecnologias em muitos países, incluindo o Brasil, reforça a urgência de políticas públicas claras e rigorosas. A regulamentação deve priorizar a proteção da privacidade e a garantia de que o reconhecimento facial seja usado de forma ética, sem comprometer a dignidade das pessoas.

Por fim, esta pesquisa reforça que o debate em torno do reconhecimento facial deve ser interdisciplinar, envolvendo governo, sociedade civil, pesquisadores e desenvolvedores. É essencial que o desenvolvimento e a aplicação dessas tecnologias sejam pautados pela transparência, pela inclusão e pela busca de soluções que minimizem os impactos éticos negativos.

Como sugestão para futuras pesquisas, recomenda-se a investigação de abordagens alternativas para mitigar os vieses raciais nos algoritmos e a avaliação dos impactos sociais a longo prazo do uso dessas tecnologias. Espera-se que este trabalho contribua para fomentar discussões sobre o tema e inspire ações concretas para uma sociedade mais justa, onde a tecnologia seja uma aliada na construção de cidades realmente inteligentes e inclusivas.

REFERÊNCIAS

ACESSA. Reconhecimento facial confunde gêmeos e causa transtorno com bancos e Gov.br. *ACESSA*, 11 mar. 2024. Disponível em: <https://www.acesa.com/economia/2024/03/209160-reconhecimento-facial-confunde-gemeos-e-causa-transtorno-com-bancos-e-gov-br.html>. Acesso em: 17 jul. 2024.

AZEVEDO, Fernanda. A tecnologia de reconhecimento facial em Recife, capital da democracia racial. *Brasil de Fato*, 20 jun. 2022. Disponível em: <https://www.brasildefato.com.br/2022/06/20/artigo-a-tecnologia-de-reconhecimento-facial-em-recife-capital-da-democracia-racial>. Acesso em: 3 set. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais - LGPD). *Diário Oficial da União: seção 1*, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 14 out. 2024.

BRASIL. Ministério do Desenvolvimento Regional. *Carta Brasileira para Cidades Inteligentes*. Brasília: MDR, 2020. Disponível em: <https://www.gov.br/mdr/pt-br/assuntos/desenvolvimento-regional/projeto-andus/carta-brasileira-para-cidades-inteligentes>. Acesso em: 5 abr. 2025.

BRASIL DE FATO. A tecnologia de reconhecimento facial em Recife: capital da democracia racial. *Brasil de Fato*, 20 jun. 2022. Disponível em: <https://www.brasildefato.com.br/2022/06/20/artigo-a-tecnologia-de-reconhecimento-facial-em-recife-capital-da-democracia-racial>. Acesso em: 6 mar. 2025.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. In: *Conference on Fairness, Accountability and Transparency*, 2018, Proceedings of Machine Learning Research. Disponível em: <https://proceedings.mlr.press/v81/buolamwini18a.html>. Acesso em: 11 fev. 2025.

BUOLAMWINI, Joy. A era da autorregulação das big techs acabou, diz Joy Buolamwini. *Fast Company Brasil*, 15 mar. 2024. Disponível em: <https://fastcompanybrasil.com/eventos/sxsw2024/a-era-da-autorregulacao-das-big-techs-acabou-diz-joy-buolamwini/>. Acesso em: 11 fev. 2025.

CNN BRASIL. Carnaval: capitais utilizam reconhecimento facial para procurar foragidos nas festas. *CNN Brasil*, 12 fev. 2024. Disponível em: <https://www.cnnbrasil.com.br/nacional/carnaval-capitais-utilizam-reconhecimento-facial-para-procurar-foragidos-nas-festas/>. Acesso em: 20 jul. 2024.

CONG, J. San Francisco Bans Facial Recognition Technology. *The New York Times*, 14 maio 2019. Disponível em: <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>. Acesso em: 3 ago. 2024.

CONGER, K.; Fausset, R.; Kovalski, S. F. San Francisco Bans Facial Recognition Technology. *The New York Times*, 14 maio 2019. Disponível em: <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>. Acesso em: 18 set. 2024.

CONNECTED SMART CITIES. Tecnologia de reconhecimento facial para a melhoria do transporte público. *Connected Smart Cities*, 20 fev. 2024. Disponível em: <https://portal.connectedsmartcities.com.br/2024/02/20/tecnologia-de-reconhecimento-facial-para-a-melhoria-do-transporte-publico/>. Acesso em: 26 out. 2024.

CURITIBA. Prefeitura de Curitiba usa a IA para aumentar a segurança, melhorar serviços e conversar com o cidadão. *Prefeitura de Curitiba*, 2024. Disponível em: <https://www.curitiba.pr.gov.br/noticias/prefeitura-de-curitiba-usa-a-ia-para-aumentar-a-seguranca-melhorar-servicos-e-conversar-com-o-cidadao/76247>. Acesso em: 9 jan. 2025

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO. Erro em reconhecimento facial constrange psicóloga em conferência. *Defensoria RJ*, 29 nov. 2023. Disponível em: <https://defensoria.rj.def.br/noticia/detalhes/29955-Erro-em-reconhecimento-facial-constrange-psicologa-em-conferencia>. Acesso em: 1 fev. 2025.

FAST COMPANY BRASIL. A era da autorregulação das Big Techs acabou, diz Joy Buolamwini. *Fast Company Brasil*, 13 mar. 2024. Disponível em: <https://fastcompanybrasil.com/eventos/sxsw2024/a-era-da-autorregulacao-das-big-techs-acabou-diz-joy-buolamwini/>. Acesso em: 28 mar. 2025.

G1. Curitiba usa reconhecimento facial como ferramenta na segurança pública, sem ter regulação específica; sociedade de controle crítica, especialista. *G1 Paraná*, 2 out. 2023. Disponível em: <https://g1.globo.com/pr/parana/noticia/2023/10/02/curitiba-usa-reconhecimento-facial-como-ferramenta-na-seguranca-publica-sem-ter-regulacao-especifica-sociedade-de-controle-critica-especialista.ghtml>. Acesso em: 15 jul. 2024.

G1. Inteligência artificial: mulheres negras sofrem mais erros em abordagens de reconhecimento facial do que brancos. *G1 - O Assunto*, 15 fev. 2024. Disponível em: <https://g1.globo.com/podcast/o-assunto/noticia/2024/02/15/inteligencia-artificial-mulheres-negras-sofrem-mais-erros-em-abordagens-de-reconhecimento-facial-do-que-brancos.ghtml>. Acesso em: 6 ago. 2024.

G1. San Francisco proíbe a polícia de usar reconhecimento facial. *G1 Pop & Arte*, 16 maio 2019. Disponível em: <https://g1.globo.com/pop-arte/noticia/2019/05/16/san-francisco-proibe-a-policia-de-usar-reconhecimento-facial.ghtml>. Acesso em: 12 jan. 2025.

G1 DISTRITO FEDERAL. Vídeo: turista engana sistema de reconhecimento facial em prédio; veja como funciona tecnologia. *G1 DF*, 6 jul. 2024. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2024/07/06/video-turista-engana-sistema-de-reconhecimento-facial-em-predio-veja-como-funciona-tecnologia.ghtml>. Acesso em: 18 nov. 2024.

G1 PARANÁ. Curitiba usa reconhecimento facial como ferramenta na segurança pública sem ter regulação específica; sociedade de controle, crítica especialista. *G1*, 2 out. 2023. Disponível em: <https://g1.globo.com/pr/parana/noticia/2023/10/02/curitiba-usa-reconhecimento-facial-como-ferramenta-na-seguranca-publica-sem-ter-regulacao-especifica-sociedade-de-controle-critica-especialista.ghtml>. Acesso em: 27 fev. 2025.

GALLO, M. et al. Smart cities – Ranking of European medium-sized cities. *ResearchGate*, 2007. Disponível em: https://www.researchgate.net/publication/261367640_Smart_cities_-_Ranking_of_European_medium-sized_cities. Acesso em: 12 jul. 2024.

GAUBI, Sushruta; MADHUSUDAN, R.; JOSHI, Sunil. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, v. 29, n. 7, p. 1645-1660, set. 2013. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X13000241>. Acesso em: 2 set. 2024.

GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY. *The Perpetual Line-Up: Unregulated police face recognition in America*. 2016. Disponível em: <https://www.perpetuallineup.org/>. Acesso em: 21 out. 2024.

GIFFINGER, Rudolf; FERTNER, Christian; KRAMAR, Hans; KALASEK, Robert. Smart cities – Ranking of European medium-sized cities. Viena: Centre of Regional Science, Vienna University of Technology, 2007. Disponível em: https://www.researchgate.net/publication/261367640_Smart_cities_-_Ranking_of_European_medium-sized_cities. Acesso em: 13 dez. 2024.

GONÇALVES, Tâmara Freitas; LIMA, Thamy Ayane França. Reconhecimento facial e racialização da suspeição: a experiência da população negra em espaços públicos. *Psicologia & Sociedade*, v. 33, e228410, 2021. Disponível em: <https://www.scielo.br/j/psoc/a/wJFV8yjBBr7cYnm3q6SXDjF>. Acesso em: 24 mar.2025.

GRYFO. Tendências do reconhecimento facial em 2025. *Blog Gryfo*, 10 fev. 2025. Disponível em: <https://gryfo.com.br/blog/2025/02/10/tendencias-do-reconhecimento-facial-em-2025/>. Acesso em: 2 abr. 2025.

HE, K. et al. Deep residual learning for image recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, p. 770–778, 2016. Disponível em: https://www.cv-foundation.org/openaccess/content_cvpr_2016/papers/He_Deep_Residual_Learning_CVPR_2016_paper.pdf. Acesso em: 16 jan. 2025.

HUMAN RIGHTS WATCH. China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App. *HRW*, 1 maio 2019. Disponível em: <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass>. Acesso em: 12 ago. 2024.

IBM. *Tendência e risco de viés algorítmico*. IBM Brasil, 2024. Disponível em: <http://ibm.com/br-pt/think/topics/algorithmic-bias>. Acesso em: 22 mar. 2025.

JAIN, Anil K.; ROSS, Arun A.; NANDAKUMAR, Karthik. *Introduction to Biometrics*. Nova Iorque: Springer, 2011. Disponível em: <https://link.springer.com/book/10.1007/978-0-387-77326-1>. Acesso em: 12 ago.2024.

JUSBRASIL. Reconhecimento facial em sistemas de segurança pública no Brasil: legalidade e ética em debate. *Jusbrasil*, 2024. Disponível em: <https://www.jusbrasil.com.br/artigos/reconhecimento-facial-em-sistemas-de-seguranca-publica-no-brasil-legalidade-e-etica-em-debate/2557159610>. Acesso em: 10 mar. 2025.

KOMNINOS, N. Smart Cities. In: WARDROP-FRUIIN, N.; MONTFORT, N. (Ed.). *The SAGE Encyclopedia of the Internet*. Thousand Oaks: SAGE Publications, 2018. Disponível em: https://www.komninos.eu/wp-content/uploads/2017/08/2018-Smart-Cities-Komninos-The-SAGE-encyclopedia-of-the-internet-3v_i8183.pdf. Acesso em: 17 fev. 2025.

KRISHNA, Suresh V.; KRISHNA, Ramesh. Issues related to face recognition accuracy varying based on race and skin tone. *ResearchGate*, 2020. Disponível em: https://www.researchgate.net/publication/342793905_Issues_Related_to_Face_Recognition_Accuracy_Varying_Based_on_Race_and_Skin_Tone. Acesso em: 27 mar.2025.

LEVISKY, Giselle. Inteligência artificial e urbanismo: uma revolução concreta. *LinkedIn*, 18 mar. 2025. Disponível em: <https://www.linkedin.com/pulse/intelig%C3%Aancia-artificial-urbanismo-uma-revolu%C3%A7%C3%A3o-e-concreta-levisky-18brf/>. Acesso em: 5 abr. 2025.

LI, S. Z.; JAIN, A. K. (Org.). Handbook of Face Recognition. New York: Springer, 2005. Disponível em: <https://link.springer.com/book/10.1007/978-0-387-77326-1>. Acesso em: 18 mar. 2025.

MARTINS, L. M. Reconhecimento facial e a autenticidade: uma questão de vieses étnico-raciais. *Horizontes*, SBC, 2024. Disponível em: <https://horizontes.sbc.org.br/index.php/2024/11/reconhecimento-facial-e-a-autenticidade-uma-questao-de-vieses-etnico/>. Acesso em: 5 abr. 2025.

MONROE, Ian. Issues related to face recognition accuracy varying based on race and skin tone. *ResearchGate*, 2020. Disponível em: https://www.researchgate.net/publication/342793905_Issues_Related_to_Face_Recognition_Accuracy_Varying_Based_on_Race_and_Skin_Tone. Acesso em: 25 mar. 2025.

MOTTA, Sophia. Como a inteligência artificial está transformando as cidades. *Caos Planejado*, 8 fev. 2024. Disponível em: <https://caosplanejado.com/como-a-inteligencia-artificial-esta-transformando-as-cidades/>. Acesso em: 5 abr. 2025.

NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE. *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*. Washington, DC: The National Academies Press, 2024. Disponível em: <https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance>. Acesso em: 5 abr. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *NIST publishes 2020 cybersecurity and privacy annual report*. Gaithersburg, MD: NIST, 2021. Disponível em: <https://csrc.nist.gov/news/2021/nist-publishes-2020-cybersecurity-and-privacy-program>. Acesso em: 4 abr. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *NIST publishes 2020 cybersecurity and privacy program annual report*. Computer Security Resource Center, 30 set. 2021. Disponível em: <https://csrc.nist.gov/news/2021/nist-publishes-2020-cybersecurity-and-privacy-program>. Acesso em: 5 abr. 2025.

NAUTILUS SUSTENTÁVEL. Sensores IoT: revolução sustentável na gestão hídrica. *Nautilus Sustentável*, 4 dez. 2024. Disponível em: <https://nautilussustentavel.com.br/sensores-iot-revolucao-sustentavel-na-gestao-hidrica/>. Acesso em: 2 abr. 2025.

NEC Brasil. Tecnologias que modernizam a segurança nas cidades inteligentes. *Blog NEC*, 2024. Disponível em: <https://blog.nec.com.br/tecnologias-que-modernizam-a-seguranca-nas-cidades-inteligentes>. Acesso em: 15 jan. 2025.

NETFLIX. *Coded Bias*. Direção: Shalini Kantayya. [S. l.]: Netflix, 2020. 1 vídeo (1h 26min). Documentário. Disponível em: <https://www.netflix.com/watch/81328723>. Acesso em: 19 mar. 2025.

ODIA. Foto de Michael B. Jordan é utilizada em catálogo para reconhecimento de suspeitos de chacina no Ceará. *O Dia*, 26 jan. 2022. Disponível em: <https://odia.ig.com.br/brasil/2022/01/6312471-foto-de-michael-b-jordan-e-utilizada-em-catalogo-para-reconhecimento-de-suspeitos-de-chacina-no-ceara.html>. Acesso em: 27 fev. 2025.

ONU BRASIL. ONU-Habitat: população mundial será 68% urbana até 2050. *Nações Unidas Brasil*, 1 jul. 2022. Disponível em: <https://brasil.un.org/pt-br/188520-onu-habitat-popula%C3%A7%C3%A3o-mundial-se-r%C3%A1-68-urbana-at%C3%A9-2050>. Acesso em: 5 abr. 2025.

PORTAL CONNECTED SMART CITIES. Tecnologia de reconhecimento facial para a melhoria do transporte público. *Connected Smart Cities*, 20 fev. 2024. Disponível em: <https://portal.connectedsmartcities.com.br/2024/02/20/tecnologia-de-reconhecimento-facial-para-a-melhoria-do-transporte-publico/>. Acesso em: 3 abr. 2025.

PREFEITURA MUNICIPAL DE CURITIBA. Prefeitura de Curitiba usa a IA para aumentar a segurança, melhorar serviços e conversar com o cidadão. *Prefeitura de Curitiba*, 4 mar. 2025. Disponível em: <https://www.curitiba.pr.gov.br/noticias/prefeitura-de-curitiba-usa-a-ia-para-aumentar-a-seguranca-melhorar-servicos-e-conversar-com-o-cidadao/76247>. Acesso em: 14 jul. 2024

RAMALHO, João Pedro Vicente. Reconhecimento Facial e a Autenticidade: a questão de vieses étnicos. *SBC Horizontes*, 3 nov. 2024. Disponível em: <https://horizontes.sbc.org.br/index.php/2024/11/reconhecimento-facial-e-a-autenticidade-de-uma-questao-de-vieses-etnico/>. Acesso em: 24 jul. 2024

SCHROFF, Florian; KALENICHENKO, Dmitry; PHILBIN, James. FaceNet: a unified embedding for face recognition and clustering. *arXiv preprint*, arXiv:1503.03832, 2015. Disponível em: <https://arxiv.org/abs/1503.03832>. Acesso em: 05 ago. 2024

SCIELO. A ética no uso de tecnologias de reconhecimento facial e suas implicações sociais. *Psicologia & Sociedade*, 2020. Disponível em: <https://www.scielo.br/j/psoc/a/wJFV8yJBBr7cYnm3q6SXDjF>. Acesso em: 11 ago. 2024

SILVA, J. Sensores IoT: revolução sustentável na gestão hídrica. *Nautilus Sustentável*, 2023. Disponível em: <https://nautilusustentavel.com.br/sensores-iot-revolucao-sustentavel-na-gestao-hidrica/>. Acesso em: 14 ago. 2024

SILVA, João. Reconhecimento facial em sistemas de segurança pública no Brasil: legalidade e ética em debate. *Jusbrasil*, 4 abr. 2025. Disponível em: <https://www.jusbrasil.com.br/artigos/reconhecimento-facial-em-sistemas-de-seguranca-publica-no-brasil-legalidade-e-etica-em-debate/2557159610>. Acesso em: 5 abr. 2025.

SOUZA, R. Como a inteligência artificial está transformando as cidades. *Caos Planejado*, 2023. Disponível em: <https://caosplanejado.com/como-a-inteligencia-artificial-esta-transformando-as-cidades/>. Acesso em: 14 ago. 2024

SUTCU, Y.; TRESSET, C.; EROL, B.; HASSAN, M. A survey on automated face recognition. *Future Generation Computer Systems*, v. 29, n. 3, p. 617–640, 2013. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0167739X13000241>. Acesso em: 18 ago. 2024

SZEGEDY, C. et al. Going deeper with convolutions. *arXiv preprint arXiv:1409.4842*, 2015. Disponível em: <https://arxiv.org/abs/1503.03832>. Acesso em: 22 set. 2024

THE VERGE. Dutch regulator fines Clearview AI over GDPR violations. *The Verge*, 3 set. 2024. Disponível em: <https://www.theverge.com/2024/9/3/24234879/dutch-regulator-gdpr-clearview-ai-fine>. Acesso em: 03 out. 2024.

TIME. Wrongfully arrested: how facial recognition technology led to an innocent man's arrest. *Time*, 10 nov. 2022. Disponível em: <https://time.com/6991818/wrongfully-arrested-facial-recognition-technology-essay/>. Acesso em: 26 out. 2024

U.S. Commission on Civil Rights. The Civil Rights Implications of the Federal Use of Facial Recognition Technology. *USCCR*, 2024. Disponível em: <https://www.usccr.gov/news/2024/us-commission-civil-rights-releases-report-civil-rights-implications-federal-use-facial>. Acesso em: 30 out. 2024

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados - GDPR). *EUR-Lex*, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>. Acesso em: 12 nov. 2024

WILLIAMS, Porcha. I was wrongfully arrested because of facial recognition. *TIME*, 6 fev. 2024. Disponível em: <https://time.com/6991818/wrongfully-arrested-facial-recognition-technology-essay/>. Acesso em: 28 dez. 2024

ZHAO, W.; CHELLAPPA, R.; ROSENFELD, A.; PHILLIPS, P. J. Face Recognition: A Literature Survey. *ACM Computing Surveys*, 2003. Disponível em: https://www.researchgate.net/publication/220566092_Face_Recognition_A_Literature_Survey. Acesso em: 20 jan. 2025