Imagem gerada por IA.

Segurança sem vigilância arbitrária:
os limites éticos da IA em cidades inteligentes.

Artigo escrito por Maria Eva Mit Lazarin.

Minibio: Empreendedora e pesquisadora. Está a frente de empresas de tecnologia e investimento, preside o Conselho Consultivo da ABRIA - Associação Brasileira de Inteligência Artificial e conselheira do AI Safety Brasil.

Junho de 2026

A cidade inteligente pode usar inteligência artificial para apoiar políticas de segurança pública, mas deixa de ser democrática quando transforma todo cidadão em suspeito permanente por meio de biometria, predição comportamental ou bases de dados pouco transparentes.

Uma cidade inteligente é também uma cidade instrumentada, medida em tempo real e governada por dados. Embora essa infraestrutura tecnológica possa ampliar a eficiência urbana, ela também abre espaço para o risco de um panoptismo digital, no qual a observação contínua se torna parte invisível da gestão da vida cotidiana [1]. Nesse sentido, as smart cities não são neutras: elas classificam

comportamentos, definem o que é considerado “bom” ou “mau” funcionamento urbano e podem produzir novas formas de disciplina social [2].

Nesse cenário, ganha relevância o conceito de justiça de dados. A justiça de dados busca estabelecer parâmetros éticos para um mundo em crescente digitalização, compreendendo a justiça como a forma pela qual as pessoas são tornadas visíveis, representadas e tratadas em razão da produção de seus dados digitais [3]. A ética, nesse contexto, exige que os cidadãos tenham algum poder sobre sua própria visibilidade e que minorias e grupos vulneráveis não sejam submetidos a uma “visibilidade disciplinar”.

Isso significa que o engajamento com a tecnologia também deve incluir a liberdade de não usar determinadas tecnologias ou de recusar que os próprios dados sejam convertidos em subprodutos de bases comerciais mantidas por grandes empresas. A justiça de dados exige, ainda, mecanismos de contestação contra discriminações baseadas em dados, especialmente quando decisões automatizadas impactam direitos, oportunidades e acesso a serviços públicos. À medida que algoritmos e redes neurais se tornam mais complexos e opacos, o caminho ético exige que governos e instituições criem mecanismos de auditoria, responsabilização e penalização da discriminação algorítmica, sem transferir todo o ônus da proteção apenas ao indivíduo.

No campo da inclusão, em vez de planejar sistemas de dados a partir da figura abstrata do “cidadão médio”, uma abordagem ética começa perguntando quais princípios de justiça podem proteger os grupos mais vulneráveis da sociedade na mesma medida em que protegem os demais. Isso implica reconhecer que todos devem ter liberdades reais de oportunidade: a possibilidade concreta de alcançar bem-estar, circular, acessar serviços e participar do funcionamento urbano que valorizam. Também implica assegurar participação cidadã efetiva no debate sobre quais tecnologias devem ou não ser implementadas nos espaços urbanos. Do contrário, a participação pode se tornar apenas uma legitimação simbólica de plataformas urbanas já previamente desenhadas por governos e fornecedores tecnológicos [4].

Muito antes de a IA generativa ganhar centralidade no debate público, estudos já demonstravam disparidades relevantes em sistemas comerciais de classificação facial. Em 2018, Buolamwini e Gebru apontaram maiores taxas de erro para mulheres de pele mais escura, evidenciando a necessidade de discutir o viés interseccional em visão computacional [5].

Muitas discussões jurídicas ou filosóficas tratam o erro em reconhecimento facial de forma genérica, como se “viés” ou “imprecisão” fossem categorias homogêneas. No entanto, os impactos práticos dependem criticamente do tipo de erro produzido pelo sistema. O falso positivo ocorre quando o sistema

associa incorretamente duas pessoas diferentes, podendo gerar abordagens indevidas, investigações injustificadas e falsas acusações. Já o falso negativo ocorre quando o sistema falha em reconhecer a mesma pessoa, o que tende a gerar inconveniências operacionais, como bloqueios ou falhas de autenticação. Estudos técnicos indicam que as taxas de falso positivo podem variar de forma expressiva entre grupos demográficos, o que torna o reconhecimento facial particularmente sensível em contextos policiais [6].

Por isso, tratar o tema apenas sob a ótica jurídica ou filosófica pode levar a regulações ineficazes ou a banimentos baseados em premissas técnicas incompletas. Ao mesmo tempo, uma leitura puramente técnica também é insuficiente. As auditorias de reconhecimento facial exigem cuidado ético, pois o próprio processo de teste pode reforçar danos se a coleta, o consentimento, a representatividade e a finalidade de uso dos dados forem mal desenhadas [7]. Além disso, bancos de dados biométricos pouco regulados podem produzir formas permanentes de vigilância, nas quais indivíduos passam a compor uma espécie de "fila de reconhecimento" contínua, mesmo sem relação concreta com atividades ilícitas [8].

Os riscos não se limitam ao reconhecimento facial. Algoritmos de policiamento preditivo podem retroalimentar o policiamento excessivo em áreas pobres ou racializadas, porque aprendem com dados históricos já enviesados. Quando registros policiais refletem práticas discriminatórias, seletivas ou ilegais, eles contaminam os sistemas preditivos. Assim, a IA não corrige uma instituição enviesada; ao contrário, pode automatizar seu passado e projetá-lo como futuro provável [9][10].

Esse ponto é essencial para evitar uma abordagem ingênua de "corrigir o algoritmo". A justiça algorítmica não é apenas um problema matemático, mas um problema sociotécnico, institucional e político [11][12][13]. Sistemas automatizados aplicados a populações vulneráveis podem ampliar punições, exclusões e formas de vigilância administrativa, especialmente quando operam sem transparência, sem devido processo e sem canais efetivos de contestação [14].

No Brasil, o PL 2338/2023, que trata do marco legal da inteligência artificial, constitui o eixo jurídico central desse debate. A proposta, aprovada no Senado e remetida à Câmara dos Deputados, permanece em discussão legislativa. O próprio debate institucional revelou a necessidade de aperfeiçoar a estrutura de governança da IA, inclusive em razão de questões relativas às competências da Autoridade Nacional de Proteção de Dados e à criação de um sistema nacional de desenvolvimento, regulação e governança da inteligência artificial [15][16].

Quando comparado ao modelo europeu, o debate brasileiro ganha contornos ainda mais relevantes. O EU AI Act estabelece limites rígidos para determinadas práticas, como social scoring, predição individual

de criminalidade, raspagem indiscriminada de imagens para bases faciais e identificação biométrica remota em espaços públicos, enquadrando-as como práticas proibidas ou fortemente restritas [17]. Essa comparação é útil para o Brasil porque evidencia a necessidade de diferenciar inovação legítima de vigilância desproporcional.

Enquanto as questões legislativas avançam, iniciativas concretas de reconhecimento facial já vêm sendo implementadas no país. O mapeamento da Defensoria Pública da União e do Centro de Estudos de Segurança e Cidadania indica a existência de centenas de projetos ativos de reconhecimento facial no Brasil, com impacto potencial sobre dezenas de milhões de pessoas, além de riscos relacionados a erro, privacidade, discriminação e ausência de controle externo [18].

Outro caso relevante é o Smart Sampa, em São Paulo. A Prefeitura descreve o programa como um sistema de monitoramento com reconhecimento facial e câmeras inteligentes, integrando câmeras públicas e privadas para ampliar a pronta resposta em ocorrências urbanas [19]. O caso explicita a fronteira delicada entre segurança pública, desejada pelos cidadãos, e vigilância massiva público-privada, especialmente quando a expansão geográfica do sistema depende da integração com redes privadas de monitoramento.

A segurança pública mediada por IA só é legítima quando é necessária, proporcional, auditável, contestável e democraticamente supervisionada. Fora desses limites, reconhecimento facial, policiamento preditivo e integração massiva de bases urbanas podem converter a cidade inteligente em uma infraestrutura de vigilância arbitrária.

Referências

[1] KITCHIN, Rob. “The real-time city? Big data and smart urbanism.” 2014.

[2] VANOLO, Alberto. “Smartmentality: The Smart City as Disciplinary Strategy.” 2014.

[3] TAYLOR, Linnet. “What is data justice?” 2017.

[4] CARDULLO, Paolo; KITCHIN, Rob. Estudos sobre smart citizenship e participação cidadã em smart cities. 2019.

[5] BUOLAMWINI, Joy; GEBRU, Timnit. “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.” 2018.

[6] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. NIST. “Face Recognition Vendor Test Part 3: Demographic Effects.” 2019.

[7] RAJI, Inioluwa Deborah et al. “Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing.” 2020.

[8] GARVIE, Clare; BEDOYA, Alvaro; FRANKLE, Jonathan. “The Perpetual Line-Up.” Georgetown Law Center on Privacy & Technology. 2016.

[9] LUM, Kristian; ISAAC, William. “To Predict and Serve?” 2016.

[10] RICHARDSON, Rashida; SCHULTZ, Jason; CRAWFORD, Kate. “Dirty Data, Bad Predictions.” 2019.

[11] BAROCAS, Solon; SELBST, Andrew. “Big Data’s Disparate Impact.” 2016.

[12] CITRON, Danielle; PASQUALE, Frank. “The Scored Society: Due Process for Automated Predictions.” 2014.

[13] SELBST, Andrew et al. “Fairness and Abstraction in Sociotechnical Systems.” 2019.

[14] EUBANKS, Virginia. “Automating Inequality.” 2018.

[15] BRASIL. Projeto de Lei nº 2338/2023.

[16] BRASIL. Proposta de Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial.

[17] UNIÃO EUROPEIA. EU AI Act.

[18] DEFENSORIA PÚBLICA DA UNIÃO; CESeC. “Mapeando a Vigilância Biométrica.” 2025.

[19] PREFEITURA DE SÃO PAULO. Programa Smart Sampa.