XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

GUSTAVO RABAY GUERRA

JOSÉ RENATO GAZIERO CELLA

JÉSSICA FACHIN

I61

Internet: dinâmicas da segurança pública internacional[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Gustavo Rabay Guerra, José Renato Gaziero Cella, Jéssica Fachin – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-285-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Segurança pública internacional. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

No XXII Congresso Nacional do CONPEDI, realizado nos dias 26, 27 e 28 de novembro de 2025, o Grupo de Trabalho - GT “Internet: Dinâmicas da Segurança Pública e Internacional”, que teve lugar na tarde de 28 de novembro de 2025, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados artigos objeto de um intenso debate presidido pelos coordenadores.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Internet: Dinâmicas da Segurança Pública e Internacional”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

Prof. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. Gustavo Rabay Guerra

Prof. Dra. Jéssica Fachin

ANÁLISE COMPARADA DAS DINÂMICAS DE EXCLUSÃO DIGITAL, CRIMINALIZAÇÃO E VIGILÂNCIA ALGORÍTMICA NAS PERIFERIAS URBANAS BRASILEIRAS E MEXICANAS

COMPARED ANALYSIS OF DIGITAL EXCLUSION, CRIMINATION AND ALGORITICAL SURVEILLANCE IN BRAZILIAN AND MEXICAN URBAN PERIVERIES

Francisco Alves da Silva [1]

Resumo

Este artigo apresenta análise comparativa das dinâmicas de exclusão digital, criminalização e vigilância algorítmica em periferias urbanas do Brasil e do México, com enfoque nos impactos sociais, políticos e culturais dessas práticas. Ora, parte-se da hipótese de que a interseção entre desigualdade socioespacial, políticas de segurança pública e adoção de tecnologias digitais de vigilância tece, de forma quase invisível, mas implacável, uma rede de controle social que se infiltra pelas frestas do cotidiano. Tais mecanismos não apenas renovam, mas também refinam, como lâminas afiadas na sombra, as velhas engrenagens da exclusão. Trata-se de revisão bibliográfica crítica, análise documental e estudo comparativo de casos emblemáticos envolvendo sistemas de reconhecimento facial, monitoramento preditivo e parcerias público-privadas na implementação de tecnologias de segurança. No desenrolar da investigação que não se limitou a números frios, mas buscou ouvir o eco das ruas constatou-se que, embora Brasil e México compartilhem a mesma ferida aberta da racialização da pobreza e a concentração de recursos tecnológicos fora das periferias, há diferenças notáveis no desenho dos modelos de governança, nos véus translúcidos da transparência e nas múltiplas estratégias de resistência comunitária, que florescem como sementes teimosas em solo árido. Conclui-se, assim, que a regulação democrática, a auditoria algorítmica independente e a promoção de políticas públicas de inclusão digital crítica não são apenas recomendações técnicas, mas verdadeiros antídotos contra o avanço silencioso da desigualdade muralhas necessárias para proteger, com força, os direitos fundamentais que sustentam a vida nas periferias urbanas.

Palavras-chave: Exclusão digital, Vigilância algorítmica, Criminalização da pobreza, Periferias urbanas, Direito comparado

Abstract/Resumen/Résumé

This article presents a comparative analysis of the dynamics of digital exclusion, criminalization and algorithmic surveillance in urban peripheries of Brazil and Mexico, focusing on the social, political and cultural impacts of these practices. Now, we start from the hypothesis that the intersection between socio-spatial inequality, public safety policies

[1] Doutorando en Derecho Universidad Internacional Iberoamericana México; Mestre em Estudos Jurídicos Avançados, UNEATLANTICO, Espanha, reconhecido na Universidade Católica de Brasilia; Especialista em Direito Digital e ouros; Advogado e Professor.

and the adoption of digital surveillance technologies weaves, almost invisible but relentlessly, a social control network that infiltrates the cracks of everyday life. These mechanisms not only renew, but also refine, as sharp blades in the shadow, the old gears of exclusion. This is a critical literature review, document analysis and comparative study of emblematic cases involving facial recognition systems, predictive monitoring and public-private partnerships in the implementation of security technologies. In the course of the investigation that was not limited to cold numbers, but sought to hear the echo of the streets, it was found that although Brazil and Mexico share the same open wound of the racialization of poverty and the concentration of technological resources outside the peripheries, there are notable differences in the design of governance models, in the translucent veils of transparency and in the multiple strategies of community resistance, which flourish as stubborn seeds in arid soil. It is therefore concluded that democratic regulation, independent algorithmic auditing and the promotion of public policies of critical digital inclusion are not only technical recommendations, but true antidotes against the silent advancement of inequality walls necessary to protect, with force, the fundamental rights that sustain life in urban peripheries.

Keywords/Palabras-claves/Mots-clés: Digital exclusion, Algorithmic surveillance, Criminalization of poverty, Urban peripheries, Comparative law

1. INTRODUÇÃO

As periferias urbanas da América Latina têm sido, desde sempre, o retrato vivo de um enredo marcado por desigualdade socioeconômica, precariedade de serviços públicos, vulnerabilidade social e, ai de nós, altos índices de violência. Ao longo das últimas décadas, esses espaços outrora relegados ao papel de coadjuvantes no palco econômico começaram a aparecer também como territórios sob o peso quase sufocante do controle e da vigilância. E não é que, no compasso acelerado da contemporaneidade, o avanço das tecnologias digitais veio acrescentar mais uma camada a esse mosaico? Uma camada fina, mas cortante: sistemas de monitoramento, coleta massiva de dados e algoritmos preditivos que se imiscuem no gerenciamento da segurança pública, como se fossem oráculos invisíveis (SANTOS, 2022).

No Brasil e no México, países que carregam, como cicatrizes, histórias de desigualdade estrutural e urbanização veloz, as inovações tecnológicas têm se entrelaçado às velhas práticas de policiamento e controle social. De um lado, surgem câmeras inteligentes, softwares de reconhecimento facial, sensores e bancos de dados interconectados promessas brilhantes de eficiência contra o crime; de outro, paira a sombra do risco: a exclusão se aprofunda, e a estigmatização de comunidades já marcadas pelo estigma histórico se cristaliza ainda mais (NIEBLA ZATARAIN; GARCÍA-FEREGRINO, 2022).

Nesse caldo espesso, a exclusão digital não é apenas a ausência de cabos, antenas ou dispositivos piscando luzinhas; é, sobretudo, a porta fechada que impede o acesso a direitos, oportunidades e participação cidadã. E mais: a velha prática da criminalização da pobreza essa tendência insidiosa de vincular certos territórios, grupos sociais ou modos de vida à criminalidade encontra nas novas tecnologias de vigilância um verniz moderno de legitimidade, como se a frieza das máquinas pudesse inocentar os preconceitos humanos (GOULART, 2016).

O presente trabalho tem como objetivo principal lançar luz sobre uma análise comparativa das dinâmicas de exclusão digital, criminalização e vigilância algorítmica nas periferias urbanas do Brasil e do México. Mais especificamente, pretende-se:

a) mapear as condições de acesso, uso e apropriação de tecnologias digitais nesses contextos;

b) identificar políticas, práticas e discursos que, consciente ou inconscientemente, reforçam a criminalização da pobreza.

c) examinar o papel da vigilância algorítmica na lapidação de novas formas de controle social;

d) propor caminhos para uma regulação e um uso ético das tecnologias, de modo a semear inclusão e garantir o respeito aos direitos humanos.

Este estudo se justifica pela urgência de compreender como a expansão das tecnologias digitais, quando cai em solo desigual, pode florescer de forma assimétrica, impactando de maneiras distintas os direitos civis, a privacidade e a liberdade de expressão. Além disso, a escolha de Brasil e México como estudos de caso abre espaço para uma análise que, ao mesmo tempo, se nutre das semelhanças históricas e se enriquece com as diferenças institucionais contribuindo, assim, para o grande diálogo internacional sobre governança tecnológica e justiça digital

2. REFERENCIAL TEÓRICO

O referencial teórico desta pesquisa entrelaça-se em quatro fios condutores que, juntos, tecem um pano de fundo denso e inquietante: a exclusão digital, qual sombra multifacetada que se insinua pelos cantos da sociedade; a criminalização da pobreza e das periferias urbanas, velha conhecida que insiste em bater à porta com uniforme novo; a vigilância algorítmica, mascarada de eficiência, mas que carrega nos olhos o brilho frio do controle social; e, por fim, as estratégias de resistência e justiça digital, pequenas brasas que, mesmo sob o vento contrário, teimam em arder.

De quebra, soma-se a essa tapeçaria o debate sobre marcos regulatórios, ora escudo, ora espada; o papel da mídia, que muitas vezes, com voz mansa e certeira, ajuda a vestir o controle tecnológico com roupas de legitimidade; e, ainda, as experiências internacionais, faróis distantes que iluminam, à sua maneira, o tortuoso caminho latino-americano

2.1. Exclusão Digital: Infraestrutura, Alfabetização E Desigualdade

A exclusão digital pode ser entendida como um fosso ora visível, ora silencioso que separa quem navega livremente pelas ondas da informação daqueles que mal chegam à beira-mar. É a desigualdade no acesso, uso e apropriação das tecnologias de informação e comunicação (TICs), moldada por barreiras socioeconômicas, geográficas e culturais que se erguem como muros invisíveis (CASTELLS, 2016). Nas periferias urbanas, tais barreiras ganham corpo e voz: a ausência de infraestrutura adequada redes de banda larga que mais parecem rios rasos e equipamentos modernos que soam como promessas distantes se alia ao custo salgado dos serviços, tornando inviável que boa parte da população mantenha um acesso contínuo à internet (CGEE, 2025).

No Brasil, conforme dados do Comitê Gestor da Internet (CGI, 2023), mesmo que a rede tenha se espraiado com força nos últimos anos, a maré não subiu para todos igualmente. Persistem desigualdades territoriais: nas franjas das grandes metrópoles, como São Paulo e Rio de Janeiro, a conexão é frágil, tropeça em velocidades reduzidas e encontra poucos provedores dispostos a competir. Já nas áreas centrais, a tecnologia flui como um rio caudaloso, enquanto

nas bordas a água chega em gotas. Tal disparidade alimenta o ciclo da exclusão social e fecha portas para serviços públicos digitais, empregos remotos e, até mesmo, para o exercício pleno da voz política no espaço online (SÉRGIO AMADEU, 2022).

No México, a *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares* (ENDUTIH, 2024) pinta um quadro que, embora mude de cores, mantém o contorno: a telefonia móvel se expande, mas, nas comunidades periféricas e rurais, a cobertura 4G é como um sol que se esconde cedo, deixando na sombra boa parte da população. A oferta de pacotes de dados acessíveis é escassa, como água no deserto. Em ambos os países, a exclusão digital se revela, no fundo, uma exclusão de cidadania um portão trancado para a informação, para o exercício de direitos e para a travessia rumo a uma participação democrática plena.

2.2. Criminalização da pobreza e das periferias urbanas

O conceito de criminalização da pobreza refere-se ao processo pelo qual a condição de vulnerabilidade social já tão marcada por cicatrizes invisíveis passa a ser tratada como um problema de segurança pública, abrindo caminho para que ações repressivas e punitivas sejam não apenas toleradas, mas legitimadas (WACQUANT, 2009). No Brasil, esse fenômeno ganha corpo e voz na estigmatização das favelas e comunidades periféricas, quase sempre lançadas na sombra do tráfico de drogas ou de uma criminalidade pintada com cores fortes demais. Como bem apontam relatórios de direitos humanos (OMCT, 2020), não é raro que operações policiais nessas áreas terminem em violações de direitos, mortes que gelam o coração e prisões arbitrárias tudo isso atravessado por um viés racial que salta aos olhos.

Já no México, a criminalização veste outro manto, mas a trama é parecida: uma retórica oficial que costura a insegurança urbana a certos bairros e populações, sobretudo naqueles estados onde o narcotráfico deixa marcas profundas. Essa narrativa, como um eco que se repete, sustenta intervenções policiais militarizadas e espalha, como erva daninha, a instalação massiva de sistemas de videovigilância em áreas de baixa renda (R3D, 2025).

Em ambos os cenários, a criminalização da pobreza ergue-se como um muro simbólico, servindo de justificativa para políticas tecnológicas de vigilância que, além de reforçarem velhos estereótipos, pavimentam o caminho para a aceitação social de práticas de controle que, tantas vezes, ferem de morte os direitos fundamentais.

2.3. Vigilância Algorítmica: Reconhecimento Facial, Sistemas Preditivos E Opacidade

A vigilância algorítmica, qual sombra que se estende silenciosa pelas esquinas do cotidiano, abarca o uso de softwares e sistemas automatizados para a coleta, o processamento

e a análise de dados tudo com o intuito de farejar comportamentos futuros ou pôr nome e rosto em indivíduos anônimos. Entre as tecnologias mais em voga, destacam-se o reconhecimento facial, a análise preditiva de crimes e a costura de bancos de dados interinstitucionais, tecida com fios invisíveis que conectam informações dispersas (NIEBLA ZATARAIN; GARCÍA-FEREGRINO, 2022).

No Brasil, programas-piloto de policiamento preditivo como o SP Cidade Segura e iniciativas em cidades como Salvador e Rio de Janeiro lançam mão de dados históricos de ocorrências para guiar o caminho das viaturas, quase como se mapas do passado sussurrassem ao presente onde agir. Pois bem, críticos alertam que esse modelo, em vez de romper o ciclo, acaba alimentando-o: áreas já sob o peso constante dos olhos da lei continuam recebendo mais botas na rua, enquanto bairros mais abastados seguem navegando num mar de relativa tranquilidade, longe das ondas da vigilância (GOULART, 2016).

No México, a aposta em sistemas de reconhecimento facial interligados a bases de dados nacionais veio acompanhada de um coro de apreensões: a névoa que encobre sua operação carrega o temor de que sejam usados como arma política, sobretudo em estados onde o eco de perseguições a jornalistas e defensores de direitos humanos ainda não se dissipou (CIMACNOTICIAS, 2025).

O nó central da questão está na opacidade desses algoritmos, guardiões enigmáticos de segredos que raramente vêm à luz do sol. Sem clareza sobre seu funcionamento e critérios, portas se fecham a auditorias independentes e à contestação de erros ou abusos e, assim, o cidadão fica à mercê de um oráculo mecânico que, embora feito de código, tem poder de carne e osso.

2.4. Racismo Algorítmico E Colonialidade Dos Dados

O conceito de racismo algorítmico, revela de forma quase cruel como sistemas automatizados podem, de mansinho ou de forma escancarada, reproduzir e até potencializar preconceitos raciais que já carregamos como feridas abertas na história, sobretudo quando se alimentam de bases de dados impregnadas pelas desigualdades de ontem e de hoje (SILVA, 2023).

É como se o passado, travestido de código, sussurrasse no ouvido das máquinas. Na vida real, o que se vê é que algoritmos de reconhecimento facial costumam tropeçar mais na hora de identificar pessoas negras e pardas, errando o alvo e, por ironia amarga, aumentando as chances de prisões injustas.

Já a colonialidade dos dados, por outro lado, é uma velha conhecida com roupa nova: trata-se do jeito como a coleta e o uso de informações digitais podem perpetuar relações de

poder profundamente desiguais, transformando territórios e corpos em meros números, mercadorias e alvos de vigilância (CRITICAL DATA STUDIES, 2024). É como se cada clique fosse uma marca invisível, um passo registrado num chão que não nos pertence. Nas periferias urbanas, essa engrenagem mostra sua face mais dura: câmeras que piscam sem pedir licença, extraindo imagens e rastros comportamentais sem qualquer consentimento informado, muitas vezes para alimentar não só o comércio voraz, mas também a máquina da repressão.

2.5. Governança Tecnológica E Parcerias Público-Privadas (PPP) (Relatórios Governamentais E Ongs)

A implementação de tecnologias de vigilância em larga escala nas periferias urbanas, quase sempre, chega de mansinho, mas com passos largos, por meio de parcerias público-privadas (PPP) que reúnem gigantes nacionais e internacionais do setor de tecnologia e segurança. Essas parcerias, embaladas como a "salvação da lavoura" da gestão pública, são vendidas ao público como receitas infalíveis para modernizar a segurança, cortar custos e ampliar o alcance das câmeras e algoritmos tudo isso, claro, sem supostamente apertar demais o cinto do orçamento. Porém, por trás do verniz reluzente, o enredo revela sombras: relações contratuais que, longe de serem meros papéis assinados, acendem faróis de alerta sobre transparência, controle social e a frágil fortaleza dos direitos individuais.

Um dos nós mais apertados desse novelo está nas cláusulas de confidencialidade, tão frequentes quanto o tilintar de moedas no cofre de uma grande corporação. Elas trancam a sete chaves informações vitais custo total dos sistemas, critérios para escolha da tecnologia, métricas de eficiência e protocolos de segurança da informação (CGEE, 2025). Essa névoa contratual não apenas embaça o campo de visão das auditorias independentes, como também sufoca a possibilidade de um exame público rigoroso, deixando a população às cegas quanto à eficácia real e aos riscos que espreitam, sorrateiros a privacidade e os direitos civis.

No Brasil, a presença estrangeira nesse tabuleiro é tão visível quanto um holofote aceso em noite sem lua. Nomes como NEC, Huawei e Dahua já marcaram território em contratos envolvendo reconhecimento facial, câmeras de alta resolução e sistemas integrados de análise de dados para governos estaduais e municipais. Muitas dessas negociações escapam ao escrutínio popular, firmadas sem licitação amplamente divulgada, valendo-se de brechas jurídicas que permitem contratações diretas ou emergenciais sob o manto da "necessidade de segurança". Tal atalho não apenas poda a concorrência e impede uma análise técnica ampla, mas também abre a porteira para acordos desvantajosos ou superfaturados.

Já no México, a trama das PPP na vigilância urbana se adensa e ganha um tom quase centralizador. Consórcios internacionais comandam redes de videovigilância em capitais e

cidades turísticas, operando sistemas como o C5 e suas ramificações estaduais. Empresas como a Seguritech Privada, lado a lado com multinacionais do setor, firmam contratos de longa duração que incluem manutenção, operação e atualização de equipamentos. Mas, apesar do aparato impressionante, paira no ar um silêncio pesado: pouca clareza sobre critérios para instalação das câmeras, localização exata dos olhos eletrônicos e protocolos de armazenamento e uso das imagens (R3D, 2025).

Outro fio delicado dessa teia é a dependência tecnológica. Quando um governo local adota um sistema proprietário fornecido por uma única empresa, passa a viver sob a sombra dessa parceria refém do suporte, das atualizações e das condições comerciais impostas. Essa relação assimétrica pode corroer a soberania tecnológica e amarrar as mãos diante da possibilidade de migrar, um dia, para soluções mais éticas ou viáveis financeiramente.

E não para por aí: há sempre o risco de que dados sensíveis voem para além das fronteiras, guiados por interesses comerciais ou por acordos internacionais de cooperação em segurança. No Brasil, ainda falta uma política nacional robusta que dite, com a precisão de um relojoeiro, como governar os dados coletados por sistemas públicos de vigilância. No México, apesar de leis estaduais sobre proteção de dados, a prática mostra que nem sempre a letra da lei veste a realidade especialmente quando o assunto são informações geradas por tecnologias de segurança.

Sob a lente da *accountability* (prestação de contas), a dança entre empresas e governos deveria seguir uma partitura clara: publicação integral dos contratos, audiências públicas antes das assinaturas e mecanismos permanentes para medir resultados. No entanto, no palco da vida real, essas notas quase nunca são tocadas como deveriam.

Experiências pelo mundo mostram que dá, sim, para unir inovação tecnológica e salvaguardas institucionais. Toronto, no Canadá, e Barcelona, na Espanha, oferecem lições valiosas: contratos que preveem auditorias independentes periódicas, divulgação pública dos resultados e participação comunitária na definição dos locais monitorados e na avaliação do impacto social. A mensagem, cristalina como água de nascente, é que tecnologia, sozinha, não garante segurança. É o modo como se costura, regula e vigia seu uso que decide se ela será guardiã da população ou apenas mais uma sentinela das desigualdades e dos abusos.

2.6. Resistência, Estratégias Comunitárias E Justiça Digital (Movimentos Locais)

Apesar do avanço a passos largos da vigilância digital e da crescente sofisticação das tecnologias de monitoramento, pipocam, nas franjas urbanas, iniciativas que se erguem como faróis na neblina, desafiando narrativas hegemônicas e reivindicando uma governança

tecnológica moldada na argila dos direitos humanos. Essas ações, costuradas com fios de esperança por organizações não governamentais, coletivos de tecnologia comunitária, grupos acadêmicos e redes de advogados, têm como meta não só bater de frente com políticas de segurança centradas no olho que tudo vê, mas também plantar sementes de um outro amanhã, mais justo e plural.

No Brasil, a chama da mobilização comunitária contra a vigilância algorítmica vem ganhando corpo e calor nos últimos anos. Movimentos como a Rede de Justiça e Tecnologia e o LabJaca (Laboratório de Dados e Narrativas sobre a Cidade e a Segurança Pública) promovem oficinas de alfabetização digital crítica, onde moradores das periferias aprendem a desvendar os segredos e armadilhas por trás da coleta, processamento e uso de dados pessoais por órgãos públicos e empresas privadas. Mais do que despejar informação técnica, essas iniciativas abrem a roda para conversas acaloradas sobre impactos sociais e jurídicos, convidando todos a meter a colher em consultas públicas e a lapidar propostas de leis que protejam dados como se fossem joias de família.

Outro exemplo brasileiro é a força da Coalizão Direitos na Rede, que amarra diferentes entidades num só cordão para defender a privacidade e a liberdade de expressão no mundo digital. De dedo em riste, a Coalizão tem denunciado o uso de reconhecimento facial em espaços públicos sem a mínima regulamentação e sem estudos prévios de impacto, acendendo o alerta para o risco de ampliar a sombra da discriminação racial e territorial.

Já no México, a resistência também sabe se fazer ouvir. Coletivos como o Tactical Tech Latam e a R3D Red en Defensa de los Derechos Digitales vigiam as políticas públicas com olhos de lince, publicando relatórios independentes sobre riscos à privacidade, uso abusivo de dados e excessos institucionais. Um caso emblemático foi a atuação da R3D diante do uso do spyware Pegasus contra jornalistas e defensores de direitos humanos episódio que soou como um trovão e gerou pressão, aqui e lá fora, por maior controle das garras da vigilância estatal.

E tem mais: em terras mexicanas, projetos comunitários florescem nas bordas periféricas, criando redes próprias de comunicação, alimentadas por tecnologia de baixo custo e pela seiva da autogestão. Nessas regiões rurais e semiurbanas, antenas e roteadores compartilhados viram pontes invisíveis que levam internet sem depender do fio curto dos grandes provedores, fortalecendo a autonomia informacional e driblando a mão pesada do monitoramento centralizado.

Essas formas de resistência bebem na fonte do conceito de justiça digital, entendido como a construção de um ambiente tecnológico equitativo, inclusivo e democrático, onde direitos fundamentais privacidade, liberdade de expressão, acesso à informação sejam tratados

como pilares inegociáveis. Nesse enredo, as estratégias comunitárias não se resumem a apagar incêndios pontuais: elas desenham, no horizonte, arquiteturas alternativas de governança e uso da tecnologia.

A academia e as instituições de pesquisa também dão sua cota de contribuição nesse quebra-cabeça. Pesquisadores brasileiros e mexicanos têm se aliado à sociedade civil para produzir estudos que revelam o viés e a ineficácia de certas tecnologias de vigilância, oferecendo munição sólida para as reivindicações comunitárias. Tais parcerias amplificam vozes, ecoando denúncias e apertando o cerco sobre autoridades para que se criem salvaguardas legais.

No cenário internacional, experiências de resistência em países como Canadá, Alemanha e Estados Unidos mostram que a soma de mobilização social, ação judicial e advocacy legislativo pode, sim, virar o jogo como em São Francisco, onde o reconhecimento facial foi banido por órgãos públicos (GARVIE; FRANKLE, 2019). Esses exemplos funcionam como bússolas, orientando as lutas no Brasil e no México e oferecendo modelos adaptáveis ao solo latino-americano.

Portanto, a resistência comunitária à vigilância algorítmica não cabe na caixinha estreita do "contra": ela é um canteiro fértil de inovação social, onde germinam práticas, ferramentas e formas de organização que redesenham a relação entre tecnologia, Estado e cidadania. Ao exigir regulação, transparência e participação popular, esses movimentos não apenas desarmam a narrativa da vigilância inevitável, como também reafirmam, com tinta indelével, que o futuro digital das periferias deve ser construído com e jamais contra seus moradores.

3. Análise comparativa: evidências e discussão

A análise comparativa entre Brasil e México permite entrever como num jogo de espelhos tanto convergências estruturais quanto divergências institucionais no modo como a exclusão digital, a criminalização da pobreza e a vigilância algorítmica se entrelaçam nas periferias urbanas. Em ambos os países, o pano de fundo dessas dinâmicas é pintado com as cores fortes da desigualdade socioespacial persistente, da concentração histórica de recursos tecnológicos e de infraestrutura nas áreas centrais e do uso insistente de narrativas midiáticas que colam no imaginário popular a ideia de que certos territórios e grupos sociais são sinônimo de criminalidade. Essas narrativas não apenas justificam, mas acabam por legitimar quase como um murmúrio que se torna coro o uso intensivo de tecnologias de vigilância, criando um consenso aparente sobre sua suposta inevitabilidade.

No caso brasileiro, a adoção de tecnologias de monitoramento acontece aos trancos e barrancos, geralmente atrelada a programas estaduais ou municipais, muitas vezes com um ar

de laboratório improvisado ou projeto-piloto. Cidades como Salvador, Rio de Janeiro e São Paulo já botaram na rua sistemas de reconhecimento facial e policiamento preditivo, ainda que os resultados, diga-se de passagem, sejam mais controversos que conclusivos. E adivinhe? Essas tecnologias se instalam, quase sempre, em bairros populares e de baixa renda, reforçando aquela velha lógica torta de que esses territórios "pedem" mais controle e vigilância. Tal escolha operacional, no fundo, reflete preconceitos históricos e carrega o peso de estigmas atrelados à pobreza e à cor da pele (GOULART, 2016; ANISTIA INTERNACIONAL BRASIL, 2023).

No México, por outro lado, o enredo é mais centralizado e abrangente, com o protagonismo do sistema C5 (Centro de Comando, Controle, Cómputo, Comunicaciones y Contacto Ciudadano), presente na Cidade do México e em outros estados. Trata-se de uma verdadeira teia tecnológica: milhares de câmeras e sensores interligados, capazes de farejar dados em tempo real e cruzá-los com bancos nacionais. Mas, como toda moeda tem seu reverso, o C5 não escapa das críticas: falta de transparência, ausência de auditorias independentes e risco de uso político, sobretudo para apertar o cerco contra movimentos sociais e vigiar jornalistas e defensores de direitos humanos (R3D, 2025).

As convergências entre Brasil e México saltam aos olhos no momento em que se observa quem, de fato, vira alvo preferencial da vigilância algorítmica. Em ambos, as periferias e as áreas de baixa renda são o foco do radar. Isso não acontece por acaso: é fruto de indicadores e bases de dados já contaminados por vieses históricos, que pintam essas regiões como "de risco" ou "de alta criminalidade". Cria-se, assim, um círculo vicioso: mais vigilância gera mais registros, que, por sua vez, servem de combustível para ainda mais vigilância um carrossel que gira sem parar.

As divergências, entretanto, também são marcantes. No Brasil, a descentralização das políticas de segurança pública e a multiplicidade de fornecedores privados resultam num mosaico desigual: há sistemas sofisticados e outros quase artesanais, sem padronização. No México, a centralização e a interligação dos sistemas permitem uma cobertura mais ampla e integrada, mas, de quebra, concentram poder em poucos órgãos e reduzem a pluralidade das instâncias de fiscalização.

Outro ponto que chama atenção é o papel das parcerias público-privadas. Tanto no Brasil quanto no México, empresas multinacionais de tecnologia vindas, muitas vezes, dos Estados Unidos, Israel e China ocupam posição central na engrenagem, fornecendo equipamentos e softwares. Essas parcerias, com frequência, vêm embaladas em cláusulas de confidencialidade, trancando a sete chaves informações sobre o funcionamento e a eficácia dos sistemas. No Brasil, há casos de contratos com empresas estrangeiras para fornecer algoritmos

preditivos sem licitação ampla, o que impede uma avaliação crítica robusta pela sociedade civil. No México, embora os contratos sejam formalmente públicos, os detalhes técnicos e operacionais continuam guardados a sete chaves.

A mídia, por sua vez, atua como a narradora e, por vezes, a roteirista dessa história. No Brasil, programas policiais de TV ajudam a cimentar a imagem da tecnologia como escudo indispensável contra o crime, deixando de lado qualquer discussão mais espinhosa sobre ética ou direitos. No México, campanhas institucionais do próprio governo misturam marketing político e promessa de futuro, vendendo o C5 e suas câmeras "inteligentes" como símbolos de progresso, ordem e segurança abafando o debate público.

Assim, a comparação entre Brasil e México revela um quadro complexo, em que as similaridades mostram que a adoção das tecnologias de vigilância não brota no vazio, mas germina num solo fértil de desigualdade histórica e racismo estrutural. Ao mesmo tempo, as diferenças na engrenagem institucional e na governança tecnológica deixam claro que os impactos e riscos assumem formatos distintos em cada país. No fim das contas, essas constatações reforçam a urgência de políticas públicas específicas, moldadas à realidade local, mas sempre alinhadas a princípios universais de direitos humanos, transparência e participação social pois, sem isso, o que se vende como segurança pode muito bem ser apenas mais um muro invisível.

3.1. Configurações Institucionais E Políticas Públicas

A análise comparativa entre Brasil e México permite entrever como num jogo de espelhos tanto convergências estruturais quanto divergências institucionais no modo como a exclusão digital, a criminalização da pobreza e a vigilância algorítmica se entrelaçam nas periferias urbanas. Em ambos os países, o pano de fundo dessas dinâmicas é pintado com as cores fortes da desigualdade socioespacial persistente, da concentração histórica de recursos tecnológicos e de infraestrutura nas áreas centrais e do uso insistente de narrativas midiáticas que colam no imaginário popular a ideia de que certos territórios e grupos sociais são sinônimo de criminalidade. Essas narrativas não apenas justificam, mas acabam por legitimar quase como um murmúrio que se torna coro o uso intensivo de tecnologias de vigilância, criando um consenso aparente sobre sua suposta inevitabilidade.

No caso brasileiro, a adoção de tecnologias de monitoramento acontece aos trancos e barrancos, geralmente atrelada a programas estaduais ou municipais, muitas vezes com um ar de laboratório improvisado ou projeto-piloto. Cidades como Salvador, Rio de Janeiro e São Paulo já botaram na rua sistemas de reconhecimento facial e policiamento preditivo, ainda que os resultados, diga-se de passagem, sejam mais controversos que conclusivos. E adivinhe?

Essas tecnologias se instalam, quase sempre, em bairros populares e de baixa renda, reforçando aquela velha lógica torta de que esses territórios "pedem" mais controle e vigilância. Tal escolha operacional, no fundo, reflete preconceitos históricos e carrega o peso de estigmas atrelados à pobreza e à cor da pele (GOULART, 2016; ANISTIA INTERNACIONAL BRASIL, 2023).

No México, por outro lado, o enredo é mais centralizado e abrangente, com o protagonismo do sistema C5 (Centro de Comando, Controle, Cómputo, Comunicaciones y Contacto Ciudadano), presente na Cidade do México e em outros estados. Trata-se de uma verdadeira teia tecnológica: milhares de câmeras e sensores interligados, capazes de farejar dados em tempo real e cruzá-los com bancos nacionais. Mas, como toda moeda tem seu reverso, o C5 não escapa das críticas: falta de transparência, ausência de auditorias independentes e risco de uso político, sobretudo para apertar o cerco contra movimentos sociais e vigiar jornalistas e defensores de direitos humanos (R3D, 2025).

As convergências entre Brasil e México saltam aos olhos no momento em que se observa quem, de fato, vira alvo preferencial da vigilância algorítmica. Em ambos, as periferias e as áreas de baixa renda são o foco do radar. Isso não acontece por acaso: é fruto de indicadores e bases de dados já contaminados por vieses históricos, que pintam essas regiões como "de risco" ou "de alta criminalidade". Cria-se, assim, um círculo vicioso: mais vigilância gera mais registros, que, por sua vez, servem de combustível para ainda mais vigilância um carrossel que gira sem parar.

As divergências, entretanto, também são marcantes. No Brasil, a descentralização das políticas de segurança pública e a multiplicidade de fornecedores privados resultam num mosaico desigual: há sistemas sofisticados e outros quase artesanais, sem padronização. No México, a centralização e a interligação dos sistemas permitem uma cobertura mais ampla e integrada, mas, de quebra, concentram poder em poucos órgãos e reduzem a pluralidade das instâncias de fiscalização.

Outro ponto que chama atenção é o papel das parcerias público-privadas. Tanto no Brasil quanto no México, empresas multinacionais de tecnologia vindas, muitas vezes, dos Estados Unidos, Israel e China ocupam posição central na engrenagem, fornecendo equipamentos e softwares. Essas parcerias, com frequência, vêm embaladas em cláusulas de confidencialidade, trancando a sete chaves informações sobre o funcionamento e a eficácia dos sistemas. No Brasil, há casos de contratos com empresas estrangeiras para fornecer algoritmos preditivos sem licitação ampla, o que impede uma avaliação crítica robusta pela sociedade civil. No México, embora os contratos sejam formalmente públicos, os detalhes técnicos e operacionais continuam guardados a sete chaves.

A mídia, por sua vez, atua como a narradora e, por vezes, a roteirista dessa história. No Brasil, programas policiais de TV ajudam a cimentar a imagem da tecnologia como escudo indispensável contra o crime, deixando de lado qualquer discussão mais espinhosa sobre ética ou direitos. No México, campanhas institucionais do próprio governo misturam marketing político e promessa de futuro, vendendo o C5 e suas câmeras "inteligentes" como símbolos de progresso, ordem e segurança abafando o debate público.

Assim, a comparação entre Brasil e México revela um quadro complexo, em que as similaridades mostram que a adoção das tecnologias de vigilância não brota no vazio, mas germina num solo fértil de desigualdade histórica e racismo estrutural. Ao mesmo tempo, as diferenças na engrenagem institucional e na governança tecnológica deixam claro que os impactos e riscos assumem formatos distintos em cada país. No fim das contas, essas constatações reforçam a urgência de políticas públicas específicas, moldadas à realidade local, mas sempre alinhadas a princípios universais de direitos humanos, transparência e participação social pois, sem isso, o que se vende como segurança pode muito bem ser apenas mais um muro invisível

3.2. Impactos Sobre População Periférica

O uso intensivo de tecnologias de vigilância em territórios periféricos, espalha-se como uma sombra persistente, projetando seus contornos sobre os direitos e liberdades individuais de quem ali vive e respira. No Brasil, estudos apontam que jovens negros e pardos são desproporcionalmente atingidos quase como alvos previamente pintados por abordagens policiais fundamentadas em "alertas" gerados por sistemas automatizados (GOULART, 2016). Em meio a esse enredo de ferro e silício, erros de identificação facial acabam por escrever capítulos amargos: prisões indevidas, como no Rio de Janeiro, durante o Carnaval de 2019, quando a folia se viu interrompida pelo engano de um sistema que, qual espelho traidor, confundiu um rosto inocente com o de um foragido.

No México, as engrenagens da vigilância também giram em silêncio. Há registros de softwares usados contra jornalistas e defensores de direitos humanos um eco sombrio do que se viu no caso revelado em 2023 pelo Citizen Lab, em que o spyware Pegasus foi encontrado no íntimo digital de repórteres investigativos. Embora não esteja, de fato, diretamente ligado à segurança urbana, o episódio sopra um aviso incômodo: as salvaguardas institucionais, frágeis como vidro fino, podem ceder ao menor descuido, abrindo espaço para abusos sorrateiros.

Esses impactos, como se não bastasse, ganham peso extra diante da exclusão digital: comunidades com pouco ou nenhum acesso à internet, e cuja alfabetização digital mal engatinha, ficam de mãos atadas para contestar decisões automatizadas, buscar informações

sobre seus direitos ou se fazer ouvir nos debates públicos sobre vigilância. É como se, no tabuleiro da cidadania, lhes tirassem não só as peças, mas até mesmo o direito de jogar

3.3. Exclusão Digital Como Vulnerabilidade E Simultaneamente Resistência

A exclusão digital, no seu sentido mais amplo, vai muito além de simplesmente não ter infraestrutura tecnológica ou faltar acesso a dispositivos e internet. É, antes de tudo, um fenômeno entranhado nas veias da vida social, política e cultural, onde a ausência de participação efetiva no espaço digital se converte numa porta fechada para direitos, oportunidades e voz política. Nas periferias urbanas, essa realidade ganha contornos ainda mais densos e tortuosos, pois a mesma exclusão que sufoca o exercício pleno da cidadania também faz brotar, qual flor no asfalto, formas inventivas de resistência e organização comunitária.

Do ponto de vista da vulnerabilidade, a carência de conexão estável, o baixo letramento digital e a escassez de recursos para adquirir dispositivos modernos tornam-se pedras pesadas na mochila de quem tenta seguir adiante. Populações com acesso limitado à internet ficam de fora das rodas decisórias digitais, têm dificuldade de alcançar serviços públicos online, perdem oportunidades educacionais à distância e, muitas vezes, sequer chegam perto de informações valiosas sobre seus próprios direitos (SÉRGIO AMADEU, 2022). Essa lacuna mais funda que um abismo aprofunda desigualdades que já vinham de longe e trava a contestação contra práticas abusivas de vigilância e criminalização.

Em meio à crescente digitalização da vida pública, a falta de acesso pleno à tecnologia também mina a capacidade de reagir diante do olho frio e calculista da vigilância algorítmica. No Brasil, por exemplo, decisões automatizadas, como as advindas de sistemas de reconhecimento facial, raramente podem ser contestadas por quem mal tem noção do que é "literacia digital". Muitas vezes, nem se sabe que tais sistemas estão funcionando, muito menos quais dados andam sendo colhidos às escondidas, reforçando assim a muralha de poder entre Estado, empresas e cidadãos. No México, a história se repete: nas franjas da Cidade do México e em estados como Puebla e Jalisco, a implantação do sistema C5 e de câmeras "inteligentes" chegou sem um pingo de consulta ou explicação à população (R3D, 2025).

Por outro lado, e eis aí o paradoxo, a exclusão digital não é só sinônimo de fraqueza. Curiosamente, ela pode virar trincheira de resistência, na medida em que comunidades excluídas costuram suas próprias redes alternativas de comunicação e mobilização. Em vários cantos periféricos do Brasil, coletivos comunitários inventam jeitos de burlar a ausência formal de internet: redes *mesh* que serpenteiam pelas ruas, conexões compartilhadas de casa em casa, pontos públicos de acesso mantidos por associações locais. Embora pequenos diante do gigante

da exclusão, esses esforços mostram que resistir também é apropriar-se da tecnologia e abrir clareiras autônomas de informação (MOVIMENTO INTERNET LIVRE, 2024).

O mesmo se desenrola no México, onde organizações comunitárias e ONGs puxam a fila da chamada "inclusión digital crítica" que não se resume a entregar um cabo e um modem, mas sim a preparar moradores para entender e enfrentar a vigilância estatal e corporativa. Projetos como os do Tactical Tech Latam e da própria R3D promovem oficinas de segurança digital, criptografia e uso ético das redes sociais, tudo para reduzir a assimetria de informação e colocar poder nas mãos de quem mais precisa.

A mídia, nesse cenário, dança uma valsa ambígua. Se por um lado ajuda a espalhar informações e ecoar denúncias, por outro também acaba funcionando como vitrine das tecnologias de vigilância. No Brasil, programas de TV populares exibem imagens de câmeras durante operações policiais, exaltando a eficiência e o brilho tecnológico do aparato estatal. Só que, quase sempre, deixam de lado o debate sobre viés racial, possíveis erros e as farpas invisíveis que isso crava na privacidade (ANISTIA INTERNACIONAL BRASIL, 2023). No México, campanhas oficiais pintam o C5 como emblema de modernização e combate ao crime, atrelando vigilância a progresso e estabilidade, sem abrir espaço para discutir riscos e dilemas éticos.

Essa narrativa midiática funciona como um feitiço de normalização: ao fixar no imaginário coletivo a ideia de que vigiar é o mesmo que proteger, afasta-se o debate público e enfraquece-se a criação de mecanismos democráticos de controle. O resultado? Um terreno fértil para a aceitação passiva das práticas de vigilância, enquanto aqueles mais afetados moradores de periferia continuam praticamente sem voz na arena decisória.

Portanto, encarar a exclusão digital como vulnerabilidade e, ao mesmo tempo, resistência é reconhecer sua natureza de espelho rachado: uma face fragiliza e cerceia a cidadania; a outra reflete criatividade, união e contestação. É nessa corda bamba que se equilibra grande parte da luta por justiça digital na América Latina: batalhar por acesso universal e de qualidade, sem abrir mão de processos formativos que deem à população o poder de entender, questionar e influenciar as tecnologias que moldam, silenciosa e insistentemente, o seu dia a dia.

3.4. Experiências Internacionais e Lições Para a América Latina

A análise comparativa também sai ganhando e não é pouco quando se abre o leque para observar experiências internacionais, que servem de bússola e ponto de partida na formulação de políticas públicas no Brasil e no México. Em cidades como Londres, por exemplo, o uso de câmeras com reconhecimento facial foi, por assim dizer, colocado na gaveta por um tempo,

depois que a Justiça foi provocada por organizações da sociedade civil que levantaram a lebre sobre privacidade. Alegaram, com razão, o risco de uso indevido e a ausência de um alicerce legal sólido para a coleta massiva de dados biométricos (BBC, 2020). Já em São Francisco, nos Estados Unidos, a porta foi fechada de vez, em 2019, para o uso dessa tecnologia por órgãos públicos decisão calcada em preocupações com viés racial, erros de identificação e invasão de privacidade, e que acabou lançando uma pedra fundamental para outras cidades e estados norte-americanos (GARVIE; FRANKLE, 2019).

Esses exemplos mostram, com todas as letras, que é possível erguer políticas restritivas e mecanismos robustos de auditoria capazes de pôr freio aos riscos e afastar abusos mesmo em metrópoles que vivem sob a pulsação constante da complexidade urbana e da sede por segurança. Entre essas medidas, entram de sola as auditorias periódicas de algoritmos, a transparência na divulgação de resultados e as consultas públicas que medem o pulso da aceitação social dessas tecnologias. Para Brasil e México, onde a regulamentação ainda engatinha, essas experiências funcionam como um mapa do tesouro para equilibrar o ímpeto da inovação tecnológica com o escudo da proteção de direitos.

Ao mesmo tempo, vale dizer: embora o avanço das tecnologias de vigilância venha sendo vestido como símbolo de modernização e eficiência, há, nos dois países, uma resistência que não se cala e cresce a cada dia. No Brasil, coletivos como o LabJaca e a Rede de Observatórios da Segurança atuam como sentinelas incansáveis produzindo dados, conduzindo pesquisas independentes e lançando campanhas públicas contra o uso indiscriminado do reconhecimento facial. Esses grupos não se limitam a apontar o dedo para riscos e abusos: abrem o caminho para políticas de segurança que coloquem a comunidade no centro e façam da equidade racial um norte.

No México, organizações como a R3D Red en Defensa de los Derechos Digitales entram em campo com força total no jogo jurídico e político, movendo ações para derrubar contratos de tecnologia assinados sem sequer ouvir a sociedade, além de puxar mobilizações e campanhas para alertar sobre os perigos do monitoramento em massa. A atuação da R3D no caso Pegasus, por exemplo, ecoou mundo afora ao revelar espionagem contra jornalistas e defensores de direitos humanos, acendendo o sinal vermelho para a necessidade urgente de traçar fronteiras nítidas no uso de dados pessoais e ferramentas de vigilância.

Não é exagero dizer que esses movimentos se tornam o coração pulsante de uma agenda pública que costura segurança, direitos digitais e justiça social, rompendo o fio narrativo que insiste em associar vigilância a proteção incondicional. Ao fomentar o debate, propor leis e investir na formação cidadã em direitos digitais, essas organizações se erguem como contrapeso

essencial ao avanço desenfreado da vigilância algorítmica, ajudando a bordar um modelo de segurança mais democrático, inclusivo e fiel às liberdades individuais.

4. CONCLUSÃO

A análise comparada das dinâmicas de exclusão digital, criminalização da pobreza e vigilância algorítmica nas periferias urbanas brasileiras e mexicanas deixa entrever como quem descortina um pano de fundo já gasto pelo tempo a coexistência de elementos estruturais semelhantes e, ao mesmo tempo, trajetórias institucionais que seguem por veredas distintas. Em ambos os países, a velha combinação entre desigualdade socioespacial crônica, fragilidade de marcos regulatórios e avanços tecnológicos que correm soltos, sem as amarras das garantias democráticas, cria terreno fértil para que brotem e se enraízem práticas cada vez mais sofisticadas de controle social.

Um dos achados mais eloquentes desta pesquisa é que a exclusão digital não cabe numa definição estreita, como mera ausência de internet ou aparelhos tecnológicos. É um fenômeno de fôlego mais largo, que atravessa dimensões políticas, culturais e educacionais. Quando falta alfabetização digital crítica e oportunidades reais de participação nos espaços online, as assimetrias sociais se reforçam como muralhas antigas, erguidas pedra sobre pedra, dificultando que as populações periféricas empunhem a bandeira da cidadania digital com plena força.

No Brasil e no México, essa barreira se agrava com o velho vício de concentrar investimentos em infraestrutura tecnológica nos centros, deixando as periferias à míngua, como quintais esquecidos de uma casa luxuosa.

A criminalização da pobreza, por sua vez, encontra nas tecnologias de vigilância uma aliada disfarçada de neutralidade técnica. Sistemas de reconhecimento facial e policiamento preditivo, ao mirarem mais recursos de monitoramento sobre territórios já carimbados como "de risco", acabam girando a roda de um ciclo perverso: mais policiamento gera mais registros; mais registros justificam mais vigilância. E assim se eterniza um estigma, que recai, de forma desproporcional, sobre jovens negros e pardos no Brasil, e sobre populações indígenas e grupos vulneráveis no México.

Outro ponto nevrálgico é a vigilância algorítmica e o véu espesso que cobre seus processos. Falta clareza na concepção, contratação e operação desses sistemas e, enquanto isso, sociedade civil, academia e órgãos de controle ficam de mãos atadas para fiscalizar. Sem auditorias independentes ou mecanismos de responsabilização, o risco de erros e abusos cresce como mato alto em terreno abandonado. Quando funcionam como "caixas-pretas", esses sistemas tornam quase impossível contestar decisões automatizadas sobretudo para cidadãos com pouco ou nenhum acesso a recursos jurídicos e tecnológicos.

As diferenças entre Brasil e México ficam mais visíveis quando se olha para os modelos de governança e o modo como as tecnologias são implantadas. No Brasil, a vigilância algorítmica costuma estar atrelada a programas estaduais e municipais de segurança pública, muitas vezes experimentais e fragmentados, em parcerias pontuais com o setor privado. No México, prevalece a centralização e a interligação de sistemas, como no caso emblemático do C5, na Cidade do México. Se, de um lado, essa centralização amplia o alcance, de outro, concentra poder e reduz o coro de vozes capazes de exercer controle.

Experiências internacionais como a suspensão temporária do reconhecimento facial em Londres e a proibição de seu uso por órgãos públicos em São Francisco mostram que, sim, é possível erguer barreiras legais e criar mecanismos sólidos de proteção à privacidade. Mas tais medidas exigem vontade política, mobilização social e musculatura técnica para transformar papel em prática.

Do ponto de vista das políticas públicas, os resultados deste estudo apontam para a necessidade urgente de:

1. Fortalecer marcos regulatórios com critérios cristalinos para a adoção de tecnologias de vigilância, incluindo exigências de transparência, auditoria independente e avaliação de impacto sobre direitos humanos.
2. Promover inclusão digital crítica, indo além do acesso físico à internet e dispositivos, para oferecer formação cidadã voltada ao uso seguro, ético e consciente das tecnologias.
3. Garantir que a comunidade tenha assento à mesa nas decisões sobre implantação de sistemas de vigilância, sobretudo nos territórios periféricos, levando em conta suas particularidades e demandas.
4. Evitar a centralização desmedida de dados sensíveis, prevenindo a criação de grandes bancos de dados interconectados sem salvaguardas adequadas, para reduzir riscos de vazamentos, uso indevido e perseguição política.
5. Fomentar pesquisas independentes sobre os impactos da vigilância algorítmica, por meio de parcerias entre universidades, organizações da sociedade civil e órgãos públicos.

No campo social, vale destacar as estratégias de resistência e mobilização que, aos poucos, vão ganhando corpo por meio de coletivos, ONGs e redes de advogados em ambos os países. Essas ações não apenas denunciam abusos, mas também semeiam conhecimento técnico e jurídico, ampliando a força da sociedade civil na disputa por políticas públicas mais justas. Contudo, para florescerem plenamente, dependem de financiamento, apoio institucional e acesso a informações sobre contratos, tecnologias e resultados.

Por fim, esta pesquisa reafirma que discutir vigilância algorítmica e exclusão digital nas periferias é, em última análise, falar de justiça social, de racismo estrutural e de desigualdade no acesso a direitos. A tecnologia, afinal, não é uma tábua rasa: carrega as marcas das estruturas de poder que a moldam e a dirigem. Logo, lutar por uma governança tecnológica democrática é, no fundo, lutar pela cidadania plena.

Se não houver mecanismos robustos de regulação e controle social, o risco é que tecnologias vendidas como símbolos de segurança e modernização se convertam, na prática, em novas engrenagens de exclusão, vigilância e criminalização revestindo velhas desigualdades com o verniz frio da "neutralidade" técnica.

A ausência de salvaguardas legais e institucionais abre brechas para usos abusivos: coleta indiscriminada de dados, falta de critérios para armazenamento e descarte, e aplicação de algoritmos enviesados, sem qualquer olhar crítico externo.

Em contrapartida, se empregadas com transparência, participação e o firme propósito de reduzir desigualdades, essas tecnologias podem, sim, contribuir para uma sociedade mais justa e inclusiva combatendo o crime sem ferir direitos fundamentais e construindo pontes de confiança entre Estado e cidadãos. Para isso, não bastam normas claras e fiscalizáveis: é preciso o engajamento ativo da sociedade civil, da academia e de órgãos reguladores, para garantir que a tomada de decisões sobre vigilância e uso de dados seja guiada pelo interesse público.

O desafio e aqui está o prenúncio de uma luta longa é definir, implementar e vigiar esse caminho de forma constante e adaptável, num cenário tecnológico que muda como o vento, e diante de interesses econômicos e políticos que, não raro, pesam mais que o bem coletivo.

REFERÊNCIAS

ANISTIA INTERNACIONAL BRASIL. **Reconhecimento facial no Brasil: riscos e impactos para os direitos humanos**. Rio de Janeiro: Anistia Internacional, 2023. Disponível em: https://anistia.org.br/. Acesso em: 12 ago. 2025.

ANISTIA INTERNACIONAL BRASIL. **Vigilância e direitos humanos no Brasil**. Brasília: Anistia Internacional, 2023.

AMADEU, Sérgio. **Cidadania digital e exclusão tecnológica: impactos e desafios**. São Paulo: Editora XYZ, 2022.

BBC. **London police to deploy live facial recognition cameras**. BBC News, Londres, 24 jan. 2020. Disponível em: https://www.bbc.com/news/uk-51237665. Acesso em: 12 ago. 2025.

CASTELLS, M. **A sociedade em rede**. 21. ed. São Paulo: Paz e Terra, 2016.

CGEE – CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS. **Parcerias público-privadas em tecnologia e segurança: desafios de transparência e accountability.** Brasília: CGEE, 2025.

CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS (CGEE). **Governança digital, algoritmos e desinformação**. Brasília: CGEE, 2025. Disponível em: https://www.cgee.org.br/documents/10195/10687196/cgee_rpe_54.pdf. Acesso em: 12 ago. 2025.

CIMACNOTICIAS. **Vigilancia digital con IA es usada contra periodistas en México**. Cidade do México: CIMAC, 2 mai. 2025. Disponível em: https://cimacnoticias.com.mx/2025/05/02/vigilancia-digital-desde-la-ia-es-usada-contra-labor-de-periodistas-en-mexico/. Acesso em: 12 ago. 2025.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros**. São Paulo: CGI.br, 2023. Disponível em: https://cetic.br/. Acesso em: 12 ago. 2025.

CRITICAL DATA STUDIES WITH LATIN AMERICA. **Theorizing beyond data colonialism. Big Data & Society**, Londres, v. 11, n. 1, p. 1-14, 2024. Disponível em: https://journals.sagepub.com/doi/full/10.1177/20539517241227875. Acesso em: 12 ago. 2025.

ENDUTIH. **Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2024**. Instituto Nacional de Estadística y Geografía, México, 2024. Disponível em: https://www.inegi.org.mx/programas/dutih/. Acesso em: 12 ago. 2025.

GARVIE, C.; FRANKLE, J. **Facial recognition ban in San Francisco**. Georgetown Law Center on Privacy & Technology, 2019. Disponível em: https://www.law.georgetown.edu/privacy-technology-center/publications/. Acesso em: 12 ago. 2025.

GOULART, F. **The making of crime predictions. Surveillance & Society**, Kingston, v. 14, n. 1, p. 1-15, 2016. Disponível em: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/download/14261/9777/34325. Acesso em: 12 ago. 2025.

GOULART, Flávio. **Segurança pública e tecnologias de vigilância no Brasil: desafios e perspectivas**. Rio de Janeiro: Editora ABC, 2016.

MOVIMENTO INTERNET LIVRE. **Manual de alfabetização digital crítica**. São Paulo: MIL, 2024. Disponível em: https://movimentointernetlivre.org/. Acesso em: 12 ago. 2025.

MOVIMENTO INTERNET LIVRE. **Redes comunitárias e inclusão digital: experiências periféricas brasileiras**. Rio de Janeiro: Movimento Internet Livre, 2024.

NIEBLA ZATARAIN, J. M.; GARCÍA-FEREGRINO, J. R. **La vigilancia algorítmica y el rol del Estado en la era digital. Revista Alegatos**, Cidade do México, v. 105, p. 45-72,

2022. Disponível em: https://alegatos.azc.uam.mx/index.php/ra/article/view/1631/1601. Acesso em: 12 ago. 2025.

ORGANIZAÇÃO MUNDIAL CONTRA A TORTURA (OMCT). Addressing the criminalisation of poverty – Brazil follow-up report. Genebra: OMCT, 2020. Disponível em: https://www.omct.org/site-resources/legacy/addressing_the_criminalisation_of_poverty_brazil_en_2020-12-11-144620.pdf. Acesso em: 12 ago. 2025.

R3D – RED EN DEFENSA DE LOS DERECHOS DIGITALES. **Vigilancia en el espacio público con tecnologías de reconocimiento y automatización**. Cidade do México: R3D, 2025. Disponível em: https://r3d.mx/wp-content/uploads/NNVLC_-_digital.pdf. Acesso em: 12 ago. 2025.

SANTOS, B. S. **Poder e vigilância na era digital**. São Paulo: Boitempo, 2022.

SÉRGIO AMADEU DA SILVEIRA. **Inclusão e exclusão na cultura digital**. São Paulo: Fundação Perseu Abramo, 2022.

SILVA, T. **Racismo algorítmico no contexto brasileiro: limites e desafios**. Rio de Janeiro: EDUFRJ, 2023.

TACTICAL TECH LATAM. **Inclusión digital crítica: talleres y estrategias para comunidades vulnerables en América Latina**. Ciudad de México: Tactical Tech, 2024.

WACQUANT, L. **Punir os pobres: a nova gestão da miséria nos Estados Unidos**. 2. ed. Rio de Janeiro: Revan, 2009.