

Olhares insurgentes: reconhecimento facial e tecnopolíticas de resistência na Criptofunk 2024

Insurgent gazes: facial recognition and technopolitics of resistance at Criptofunk 2024

André Custódio Pecini

Pós-doutorando, PPGTU/PUCPR – Curitiba, Brasil
andrepecini@gmail.com
<https://orcid.org/0000-0002-1226-2038>

Debora Pio

Doutoranda, ECO/UFRJ – Rio de Janeiro, Brasil
deboradpio@gmail.com
<https://orcid.org/0000-0002-8125-2650>

Rubia Marafio Sehnm

Graduanda, Geografia UFPR – Curitiba, Brasil
marafigorubia@gmail.com
<https://orcid.org/0009-0007-2275-0450>

Pietra Milani Bizerril

Mestranda, PPGGEO UFPR – Curitiba, Brasil
pietrabmilani@gmail.com
<https://orcid.org/0009-0003-9828-2746>

Yasmin Marques dos Santos

Mestranda, PPGTU/PUCPR – Curitiba, Brasil
yasminmarquesa@gmail.com
<https://orcid.org/0009-0006-5895-9937>

Rodrigo José Firmino

Professor titular, PPGTU/PUCPR – Curitiba, Brasil
rodrigo.firmino@pucpr.br
<https://orcid.org/0000-0002-0831-6603>

Carolina Batista Israel

Professora, PPGGEO/UFPR – Curitiba, Brasil
carol_israel@ufpr.br
<https://orcid.org/0009-0002-1438-3439>

Gilberto Vieira

Doutorando, PPGTU/PUCPR – Curitiba, Brasil
gilbertovieiracruz@gmail.com
<https://orcid.org/0000-0002-2688-7565>

RESUMO: Este artigo relata uma experiência de ativação comunitária voltada à mobilização da sociedade civil e à discussão crítica sobre os riscos do uso do Reconhecimento Facial (RF) na segurança pública. O RF, uma tecnologia baseada em Inteligência Artificial (IA), tem se expandido no Brasil sob a promessa de eficiência e neutralidade, mas apresenta falhas significativas que resultam em prisões injustas e reforçam preconceitos estruturais. Longe de ser apenas uma ferramenta técnica, opera como agente em um processo tecnopolítico opaco de vigilância que afeta desproporcionalmente populações negras e periféricas. A ativação comunitária relatada neste artigo ocorreu no evento Criptofunk 2024, no conjunto de favelas da Maré, no Rio de Janeiro, e envolveu quatro diferentes atividades integradas: experimentação de algoritmos de Reconhecimento de Emoções; oficina com apresentação e debate sobre RF; maquiagem de resistência; performance de *graffiti* ao vivo sobre RF. O objetivo foi sensibilizar e mobilizar sociedade civil e gestores públicos para os riscos do uso do RF como instrumento de discriminação e violações da liberdade e privacidade de

cidadãos e cidadãs. Para isso, foram combinados elementos de pesquisa-ação, observação participante e experimentação sociotécnica situada, estruturados em procedimentos operacionais previamente definidos. O alto engajamento do público foi mensurado em entrevistas de caráter semiestruturado com critério intencional (*purposive sampling*), pela participação registrada na oficina-debate e também pela menção pública da ativação em evento realizado meses após sua realização indicam o êxito da proposta de conectar universidade e território, promovendo trocas horizontais, crítica social e aprendizado mútuo.

PALAVRAS-CHAVE: Reconhecimento Facial, Segurança pública, Ativação comunitária.

ABSTRACT: This article reports on a community activation experience aimed at mobilizing civil society and fostering a critical discussion about the risks associated with the use of Facial Recognition (FR) in public security. FR, a technology based on Artificial Intelligence (AI), has expanded in Brazil under the promise of efficiency and neutrality. However, it exhibits significant flaws that lead to unjust arrests and reinforce structural prejudices. Far from being just a technical tool, FR operates as an agent in an opaque technopolitical process of surveillance that disproportionately affects Black and peripheral populations. The community activation detailed in this article took place at the Criptofunk 2024 event in the Maré favela complex, Rio de Janeiro, and involved four integrated activities: experimentation with Emotion Recognition algorithms; a workshop featuring a presentation and debate on FR; resistance makeup application; and a live *graffiti* performance about FR. The objective was to raise awareness and mobilize civil society and public managers regarding the risks of using FR as an instrument of discrimination and violations of citizens' freedom and privacy. To achieve this, elements of action-research, participant observation, and situated socio-technical experimentation were combined, structured in predefined operational procedures. The high level of public engagement, measured through semi-structured interviews using purposive sampling, registered participation in the workshop-debate, and the public mention of the activation months later indicates the proposal's success in connecting the university and the territory, promoting horizontal exchanges, social critique, and mutual learning.

KEYWORDS: Facial Recognition, Public security, Community engagement.

Introdução

A experiência examinada neste artigo faz parte das iniciativas propostas no projeto “Dados e ativação comunitária sobre o uso de reconhecimento facial na segurança pública”, apoiado pela CAPES pelo edital PROEXT-PG, que busca investigar criticamente os impactos do uso de Reconhecimento Facial (RF) na segurança pública nas cidades de Curitiba e do Rio de Janeiro. O projeto articula investigação empírica, experimentação técnica e ativação comunitária, com o intuito de fomentar processos de conscientização e práticas de resistência tecnopolítica.

O projeto possui duas dimensões complementares: Monitoramento de Dados e Conscientização Comunitária. A primeira dimensão consiste na produção de um painel de monitoramento de dados sobre o uso de RF na segurança pública. Esse monitoramento depende, assim, de uma pesquisa sobre a disponibilidade e a coleta de dados sobre ocorrências policiais nas cidades selecionadas a fim de identificar correlações com a implantação dos aparatos de videomonitoramento e RF; também prevê a análise do orçamento destinado à compra e manutenção dos equipamentos usados nessas iniciativas. A segunda dimensão visa realizar ativações comunitárias sobre o Reconhecimento Facial em territórios periféricos das cidades escolhidas.

A primeira oficina de ativação, que é foco do presente trabalho, ocorreu na Criptofunk 2024, evento que reúne coletivos, pesquisadores e ativistas no Conjunto de Favelas da Maré para discutir as relações entre tecnologia, vigilância e liberdade. No evento, o projeto contribuiu com as seguintes atividades: oficinas compostas por apresentações e discussões com o público; experimentação técnica com algoritmos de Reconhecimento de Expressões Faciais, nas quais os participantes do evento tiveram suas idades, emoções, gêneros e etnias estimados por modelos de visão computacional; pintura facial, a fim de testar técnicas de maquiagem que dificultam o Reconhecimento Facial, expressando formas individuais de resistência e subversão e, por fim, uma performance de *live painting* que resultou em um mural de *grafitti* sobre vigilância e Reconhecimento Facial. A intervenção artística aconteceu na parte externa do galpão onde ocorreu o evento e chamou a atenção das pessoas que passavam na frente dele, promovendo maior interação entre o evento e a comunidade.

A metodologia adotada na oficina de ativação comunitária combinou elementos de pesquisa-ação, observação participante e experimentação sociotécnica situada, estruturando-se em procedimentos operacionais previamente definidos. O processo foi organizado em três etapas complementares. Na etapa preparatória, realizou-se a definição dos objetivos pedagógicos das atividades e o desenho dos protocolos de interação com os participantes, incluindo instruções éticas relacionadas ao uso de imagens, consentimento informado e estratégias para evitar a coleta desnecessária de dados sensíveis. Na etapa de realização das atividades, adotou-se uma abordagem dialógica em que cada oficina articulava momentos expositivos breves, debates mediados e exercícios práticos. As dinâmicas de experimentação técnica (especialmente aquelas relacionadas ao teste de algoritmos de reconhecimento de expressões faciais) seguiram um roteiro que

incluía demonstração dos modelos, abertura para que o público testasse sua própria imagem, discussão dos resultados algorítmicos e problematização de vieses e classificações automatizadas. Já as ações de “pintura facial” e “*live painting*” foram conduzidas como práticas de criação coletiva, buscando explorar como gestos estéticos podem operar simultaneamente como meios de expressão política e como tecnologias populares de contravigilância. Na etapa posterior ao evento, foram produzidos registros analíticos das interações, anotações de campo e sistematizações preliminares das percepções dos participantes, visando informar as próximas fases do projeto e orientar o desenho das oficinas subsequentes. Essa orientação metodológica buscou, em conjunto, produzir conhecimento situado, estimular formas críticas de literacia algorítmica e fortalecer capacidades coletivas de resistência tecnopolítica.

O objetivo dessas iniciativas de ativação comunitária, que tiveram lugar na Criptofunk e que seguirão ocorrendo ao longo do projeto nas cidades de Curitiba e Rio de Janeiro, é sensibilizar e mobilizar sociedade civil e gestores públicos para os riscos do uso do Reconhecimento Facial na segurança pública, como instrumento de discriminação e violações da liberdade e privacidade de cidadãos e cidadãs.

A proposta aqui desenvolvida parte do entendimento de que os dispositivos de vigilância digital, como o Reconhecimento Facial, não operam de forma neutra ou descontextualizada. Ao contrário, inscrevem-se em territórios marcados por desigualdades históricas e funcionam muitas vezes como tecnologias de controle que aprofundam processos de criminalização e exclusão. Em resposta, coletivos e iniciativas de base comunitária têm desenvolvido práticas contra-hegemônicas que articulam saberes populares, linguagem cultural e crítica tecnopolítica para enfrentar os riscos associados à vigilância algorítmica.

O Reconhecimento Facial é analisado não apenas como uma ferramenta técnica de segurança, mas como um operador sociotécnico que revela disputas em torno do controle de dados, da liberdade dos corpos e do direito à cidade. Tal abordagem exige a consideração de práticas de resistência nas margens urbanas, práticas que não apenas reagem ao controle, mas produzem alternativas políticas às formas dominantes de governança tecnológica. A Criptofunk 2024, nesse sentido, aparece como espaço privilegiado para observar e analisar essas dinâmicas de enfrentamento e criação.

O artigo está organizado em três seções principais, além desta introdução. A primeira seção discute os usos do Reconhecimento Facial na segurança pública no Brasil e a importância da conscientização comunitária sobre seus impactos, com

atenção especial ao contexto do conjunto de favelas da Maré e à proposta política da Criptofunk. A segunda seção apresenta as atividades realizadas durante o evento, detalhando as oficinas “Bota a cara”, “Passando a visão” e “Pinta a cara”, bem como a intervenção artística de *live painting*, analisando como essas ações contribuíram para a construção coletiva de sentidos críticos sobre a vigilância algorítmica. Por fim, as considerações finais retomam os principais argumentos do texto e apontam caminhos para o fortalecimento de práticas de resistência tecnopolítica em territórios periféricos.

RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

O Reconhecimento Facial (RF) é uma tecnologia de Inteligência Artificial (IA) discriminativa¹ cujo uso vem crescendo exponencialmente em diversas partes do mundo, principalmente para fins de vigilância e controle de pessoas. Na segurança pública, o RF funciona a partir de bases de dados alimentadas com imagens de pessoas “suspeitas”, conectadas às câmeras instaladas nas ruas, que procuram rostos equivalentes. Quando há uma correspondência entre as imagens do banco de dados e as imagens capturadas nas ruas, as centrais policiais são avisadas e partem para fazer a conferência ao vivo. Embora a tecnologia pareça o passo para um futuro onde as máquinas realizam trabalhos com neutralidade e extrema eficiência, os resultados apresentados até agora mostram justamente o contrário.

As câmeras utilizadas no RF para a segurança pública ainda são pouco eficazes: há até bem pouco tempo, os algoritmos empregados para fazer equivalência de rostos acertavam cerca de 10 em 100 vezes (Hao, 2020), percentual bem baixo para o emprego indiscriminado de uma tecnologia. Outro aspecto preocupante é que os algoritmos são ainda mais imprecisos quando se trata de rostos de pessoas negras, mulheres ou pessoas trans – a tecnologia tende a acertar mais quando os rostos analisados são de homens brancos. Mesmo assim, segundo dados do Panóptico, o monitor de Reconhecimento Facial no Brasil (2025), o país já conta com 408 projetos oficiais ativos, o que significa um potencial de 87 milhões de pessoas vigiadas, ainda que os algoritmos empregados não estejam totalmente de acordo com a diversidade de tipos brasileiros.

1 As IAs são usualmente classificadas como discriminativas ou generativas, de acordo com sua função. As primeiras são empregadas para filtragem e classificação de grandes conjuntos de dados (a exemplo da identificação de um determinado rosto dentro de um amplo banco de faces, como no RF), enquanto as segundas são destinadas à produção de conteúdos a partir de uma base de dados (Marques, 2023).

Mas não é só a vigilância indiscriminada o principal problema trazido pelas câmeras de Reconhecimento Facial. A falta de transparência e padronização dos equipamentos, assim como da coleta de dados, também é uma questão que pode contribuir ainda mais para o aprofundamento das desigualdades, já que não existem protocolos ou regras em comum para a instalação de câmeras de Reconhecimento Facial no Brasil. O relatório “Mapeando a Vigilância Biométrica” apresenta a informação que

cada estado adota um procedimento distinto na abordagem de pessoas identificadas pela tecnologia de reconhecimento facial e a falta de uma diretriz padrão para o uso da tecnologia nos Autos de Prisão em Flagrante (APF) (...) e essas situações podem não apenas levar a práticas discriminatórias e abusivas, mas também ameaçam os princípios constitucionais da ampla defesa e do devido processo legal (Panóptico, 2025, p.20).

As aquisições de equipamentos de RF ou videomonitoramento são, em sua maioria, realizadas em regime emergencial ou a partir de licitações sem critérios estabelecidos para a manutenção da segurança, privacidade e respeito aos direitos humanos.

Um dos exemplos que demonstra a controvérsia estabelecida pelo uso ampliado dessas tecnologias na segurança pública é o edital do Smart Sampa, projeto proposto pela Prefeitura de São Paulo para instalar 20 mil câmeras de videomonitoramento pela cidade. A primeira versão do texto² mencionava a identificação de pessoas “suspeitas” de acordo com cor, face, roupas, forma do corpo/aspecto físico, e também sobre monitorar ações de “vadiagem”. O documento foi amplamente criticado por organizações sociais, que chegaram a entrar com uma ação no Ministério Público para cancelar o edital. Na ocasião, a prefeitura suspendeu o pregão, mas depois de mais de um ano de imbróglio, o projeto teve continuidade. Segundo dados levantados pelo veículo Intercept³, o consórcio vencedor da licitação é composto por empresas envolvidas em casos de corrupção (Rebello, 2023). A prefeitura irá pagar R\$9,8 milhões por mês para o consórcio instalar as câmeras no prazo de 18 meses.

2 Após a campanha das organizações da sociedade civil que barraram o edital, o texto foi modificado e os termos que falavam sobre cor da pele, face etc foram subtraídos. No entanto, a primeira versão ainda está disponível no link: <https://participemais.prefeitura.sp.gov.br/legislation/processes/209/topics#legislation_topic_7443> (acesso em 18 de novembro de 2025).

3 Investigação realizada pelo veículo Intercept, para o especial “Quem Paga a Conta”, disponível no link: <<https://www.intercept.com.br/2023/08/14/smart-sampa-denunciada-por-corrupcao-capturar-seu-rostro-em-sp/>> (acesso em 18 de novembro de 2025).

A falta de transparência também deve ser observada, uma vez que não existem informações oficiais sobre os resultados aferidos sobre a eficiência das câmeras ou sobre a diminuição da criminalidade nas localidades onde elas estão instaladas. Muito pelo contrário: em um requerimento feito via LAI para a Secretaria de Polícia do Estado do Rio de Janeiro sobre a localização das câmeras, projetos ativos e índices verificados, a resposta foi: “a Secretaria de Estado de Polícia Militar agradece o contato e, em atenção à manifestação, deixa de disponibilizar as informações sobre câmeras de Reconhecimento Facial em operação na cidade do Rio de Janeiro, com valores agregados por bairro, pois sua divulgação pode comprometer a segurança pública e a integridade dos próprios equipamentos”. A alegação de sigilo e de que a divulgação deste tipo de informação é uma ameaça à segurança pública têm sido a resposta comum para pedidos de informação feitos por pesquisadores e sociedade civil.

Além disso, “são crescentes os relatos de pessoas presas, processadas ou investigadas com base em dados biométricos extraídos de bancos compartilhados entre diferentes instituições, sem critérios claros de acesso, revisão ou possibilidade de contestação” (Nunes, 2025). Alguns casos são amplamente midiáticos como o do personal trainer sergipano João Antônio Trindade⁴, que foi detido durante um jogo do campeonato local entre os times Confiança e Sergipe. Segundo relato, ele foi levado da arquibancada do estádio por cinco policiais após o sistema de Reconhecimento Facial apontar que ele era um foragido. Depois da PM aferir os documentos de João, foi constatado que a máquina havia cometido um erro e ele foi liberado para voltar ao jogo. Casos como este têm sido muito comuns, sobretudo com pessoas negras, depois do aumento da instalação das câmeras em espaços públicos, inclusive estádios de futebol.

Estes episódios podem ser classificados pelo que Tarcízio Silva designa como racismo algorítmico, compreendendo tal fenômeno como

o modo pelo qual a disposição de tecnologias e imaginários sociotécnicos em um mundo moldado pela supremacia branca realiza a ordenação algorítmica racializada de classificação social, recursos e violência em detrimento de grupos minorizados. Tal ordenação pode ser vista como uma camada adicional do racismo estrutural, que, além do mais, molda o futuro e os horizontes de relações de poder, adicionando mais opacidade sobre a exploração e a opressão global que já ocorriam desde o projeto colonial do século XVI (Silva, 2022, p.69).

4 A própria vítima do reconhecimento equivocado fez um relato no X (ex-Twitter). <https://x.com/joantoniotb/status/1779856876584268110> (acesso em 14 de novembro de 2025).

No caso do RF utilizado na segurança pública, as evidências mostram que o resultado é uma classificação social de indivíduos a partir dos territórios onde vivem e, principalmente, de sua cor de pele. Estes cidadãos e estas cidadãs se tornam ainda mais vulneráveis a punições e controle já engendrados pelas polícias, sem que estas pessoas tenham direito à segurança de seus dados biométricos capturados à revelia e, no caso de uma prisão ou apreensão equivocada, não terem direito a qualquer tipo de reparação.

O CONJUNTO DE FAVELAS DA MARÉ E A CRIPTOFUNK

A Criptofunk é um evento que acontece desde 2018 na Maré, um conjunto de 16 favelas localizado na zona norte do Rio de Janeiro. Segundo o Censo Maré (2019)⁵, sua população gira em torno dos 140 mil habitantes, 62,1% autodeclarados pretos ou pardos.

Sendo uma das localidades mais populosas da cidade, grande parte de seus moradores vivem em condições de vulnerabilidade causadas pela violência, pobreza e ausência de políticas públicas que deem conta de reduzir as desigualdades. Nas últimas duas décadas, o conjunto de favelas foi palco de duas grandes chacinas: uma em 2013, que deixou dez mortos, e outra em 2018, que vitimou oito pessoas. Somado a estes dados trágicos, a Maré ainda é um dos locais com maior incidência de operações policiais que resultam em mortes comparadas às outras favelas da cidade⁶.

Mas, apesar de ser um bairro constantemente noticiado pela violência, a Maré tem uma vida cultural pujante, com dois grandes centros culturais, museus, pólos gastronômicos e mais de 3.000 estabelecimentos comerciais (Censo de Empreendimentos Maré, 2014), além de ser também o local de nascimento e surgimento de potências que mudaram a história política do país, como a vereadora Marielle Franco.

É neste território que surge a Criptofunk, um evento gratuito e aberto que busca democratizar o conhecimento sobre privacidade digital, proteção de dados e justiça tecnológica, com uma abordagem territorializada e conectada à cultura

5 O Censo Maré é uma iniciativa capitaneada pela Redes da Maré, realizada em 2019 e traz dados pormenorizados do território, em complemento ao Censo regular realizado pelo IBGE. Disponível em <<https://apublica.org/wp-content/uploads/2020/07/censoma-re-web-04mai.pdf>> (acesso em 10 de novembro de 2025).

6 Boletim Direito à Segurança Pública na Maré. Disponível em: <<https://www.redesdamare.org.br/br/info/22/de-olho-na-mare>> (acesso em 10 de novembro de 2025).

popular. Com o lema “Criptografe dados, descriptografe o corpo”, o objetivo do evento é promover a autonomia e a liberdade das pessoas frente à influência das tecnologias em suas vidas, por meio da combinação entre debates, oficinas e atrações culturais.

Em um mundo em que a internet ganha cada vez mais centralidade no cotidiano de grande parte da população, as discussões sobre liberdade de expressão, privacidade na internet, algoritmos, direitos humanos e cuidados integrais (físicos, digitais e psicossociais) se tornam cada vez mais urgentes (Criptofunk, [s.d.])

A Criptofunk propõe, assim, uma intersecção entre tecnologia, cultura e ativismo, assumindo o funk (expressão musical e política das periferias) como linguagem para traduzir temas complexos relacionados à vigilância digital e ao controle algorítmico em experiências acessíveis, críticas e comunitárias. Cada edição do evento conta com a participação e organização de um conjunto de coletivos, instituições locais, ONGs voltadas a temas correlatos, universidades e fundações filantrópicas arregimentadas pelo data_labe. A organização social surgida na Maré em 2016 tem o objetivo de democratizar o acesso ao debate sobre dados e tecnologias para moradores de favelas e periferias do Brasil. A assinatura do projeto é sempre coletiva⁷ porque respeita o princípio de cocriação das Criptofestas – eventos globais voltados ao debate sobre criptografia e segurança digital na era da informação. A diferença está no caráter territorial, situado e posicionado da Criptofunk. A Maré é um território historicamente atravessado por práticas de vigilância e violência de Estado, mas também por potentes formas de resistência e (re)existência. A territorialização do debate sobre tecnologia permite que as questões tratadas, como o uso de Reconhecimento Facial, a criminalização de corpos negros e periféricos e a disputa por soberania informacional, sejam abordadas a partir das vivências concretas das populações diretamente afetadas.

A quinta edição da Criptofunk reuniu artistas, ativistas e pesquisadores em torno de uma programação de mais de 20 horas de debates, oficinas e performances sobre tecnologia, funk, corpo e suas conexões com inteligência artificial e questões de gênero, raça, direitos humanos e bem viver. Em cada atividade desta edição, o que também pode ser facilmente identificado nas outras, os participantes, ouvintes, professores, produtores ou artistas tensionavam a lógica

7 Cada uma das cinco edições da Criptofunk contou com diferentes parceiros e organizadores, com exceção do data_labe que é o eixo central de produção do evento.

tecnossolucionista, que frequentemente ignora desigualdades estruturais, propondo em seu lugar práticas tecnopolíticas situadas, insurgentes e enraizadas na cultura periférica. É possível identificar essas tensões em oficinas intituladas “Decolonize seus quadris”; “O que raios é inteligência artificial”; “Crie seu próprio algoritmo”; “Cultura como tecnologia de convivência”; ou “Tecnologias ancestrais de autocuidado”, para dar alguns exemplos. Dessa forma, a Criptofunk contribui não apenas para ampliar o debate público sobre vigilância e dados, mas também para fortalecer redes de cuidado, autonomia e justiça nas bordas do urbano.

Enquanto equipe responsável por conceber, mediar e executar as atividades do projeto de extensão que embasa este artigo, atuamos como pesquisadores-extensionistas inseridos no processo desde sua etapa de planejamento. Nossa participação envolveu o desenho pedagógico das oficinas, a coordenação das dinâmicas de discussão e experimentação sociotécnica e o acompanhamento das interações com moradores e participantes do evento. Essa posição implicada no território orientou a escolha das metodologias empregadas, permitindo articular os referenciais críticos sobre vigilância algorítmica às formas de expressão cultural e às experiências concretas vivenciadas na Maré. Assim, as ações realizadas durante a Criptofunk não apenas dialogaram com o contexto local e com o histórico de vigilância no território, como também refletiram o compromisso dos autores com práticas de extensão engajada, capazes de produzir conhecimento situado e politicamente relevante.

Em diálogo com a proposta do evento e com o contexto do território, organizamos uma série de atividades interativas de discussão, reflexão e sensibilização, sobre a crescente implementação de tecnologias de vigilância e controle, especialmente em espaços públicos e periferias urbanas.

ATIVIDADES DO PROJETO NA CRIPTOFUNK 2024

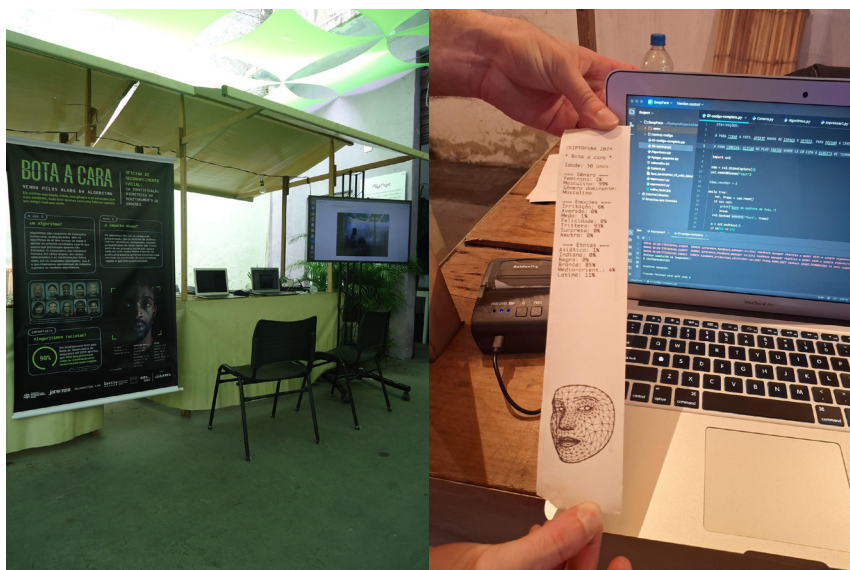
As atividades enumeradas na introdução foram o resultado da participação de diversos colaboradores e colaboradoras. Foram eles: o Jararaca (Laboratório de Tecnopolíticas Urbanas da PUCPR, coordenado por Rodrigo Firmino), o Tecnosfera Lab (UFPR, coordenado por Carolina Israel), o MediaLab.UFRJ (coordenado por Fernanda Bruno) e o data_labe (representado neste projeto por Gilberto Vieira e Elena Wesley), organizador da Criptofunk. O evento também contou com apoio da LAVITS, Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e

Sociedade, que reúne vários pesquisadores e ativistas membros desses laboratórios. A seguir, cada uma dessas atividades será detalhada.

“Bota a cara”: vendo pelos olhos do algoritmo

O principal objetivo das atividades propostas pelo projeto de extensão para a Criptofunk foi promover a conscientização comunitária acerca dos impactos do uso cotidiano das tecnologias de Reconhecimento Facial. Como primeira intervenção, foi realizada a instalação “Bota a cara: vendo pelos olhos do algoritmo”, na qual os participantes puderam experimentar diretamente o funcionamento dessa tecnologia. Nesta instalação, Rubia Marafigo Sehnem e André Custódio Pecini adaptaram algoritmos de Reconhecimento de Expressões Faciais disponibilizados pela Microsoft, pela Alphabet/Google e pela Meta/Facebook, de modo a executá-los diretamente dos computadores do projeto, sem conexão com a Internet. Seu título, “bota a cara”, comunica de forma informal o que os participantes poderiam fazer: colocar seus rostos na frente dos computadores para que as imagens capturadas pelas câmeras fossem analisadas pelos algoritmos, seja exibindo em tempo real as emoções estimadas, seja imprimindo um relatório com os pontos faciais identificados, além de estimativas de idade, gênero, etnia e emoções.

Figura 1 – Instalação “Bota a cara”. À esquerda, os equipamentos (notebooks e TV que exibia dados em tempo real) e à direita, detalhe do relatório oferecido a cada participante.



O primeiro algoritmo foi desenvolvido em linguagem de programação JavaScript⁸ para a construção de uma interface de RF de emoções, gênero e idade, a partir do algoritmo API de Detecção Facial da Microsoft. A partir desse algoritmo e com base nos tutoriais de Castiglioni (2020) e Schiffler (2021), pode-se identificar rostos em tempo real, primeiramente realizando um mapeamento de olhos, nariz, boca e contorno, formando uma malha facial. Posteriormente, o sistema estima idade, gênero e expressões faciais. No segundo experimento, foram combinadas duas abordagens do reconhecimento de expressões faciais e emoções. Uma delas foi a biblioteca DeepFace, desenvolvida por pesquisadores da Meta (ex-Facebook) que encapsula diversos dos principais modelos de Reconhecimento Facial e de Expressões Faciais – VGG-Face, Facenet, OpenFace, Dlib, entre outros (Taigman et al., 2014). Além dela, também foi usado o *MediaPipe Face Landmarker*, um modelo desenvolvido pela Alphabet/Google que detecta pontos de referência do rosto e expressões faciais e pode ser usado para “identificar expressões faciais humanas, aplicar filtros e efeitos faciais e criar avatares virtuais” (Google, [s.d.]), que gera a imagem da malha facial com os pontos identificados.

A proposta permitiu vivenciar os mecanismos operacionais do Reconhecimento Facial, uma vez que os participantes interagiram diretamente com dois sistemas diferentes durante a instalação. Ao se prestarem diante da câmera do computador, acompanhavam a formação da própria malha facial identificada pelos algoritmos, e posteriormente a partir desse resultado, foram classificados idade, gênero, etnia e expressões faciais. Essa experiência prática possibilitou observar como os sistemas processam o rosto, as etapas que compõem a análise e como as decisões algorítmicas são produzidas (processo explicado aos participantes e detalhado abaixo), com base na identificação automatizada de pontos faciais e sua comparação com modelos gerados a partir de bases de dados de milhões de faces. Assim, os participantes puderam experimentar em primeira mão e de forma crítica as falhas e os vieses que esses sistemas reproduzem.

Neste sentido, a percepção das falhas e dos vieses ocorreu juntamente na experimentação técnica dos sistemas. Testes feitos pelos próprios participantes, como alterar a expressão facial, cobrir partes do rosto e variar a distância, evidenciaram os erros de detecção mencionados. No que tange os vieses algorítmicos, estes puderam ser compreendidos nas inconsistências na leitura de diferentes

8 Trata-se de uma linguagem de programação leve e de uso geral, seus principais usos destinam-se ao desenvolvimento web e desenvolvimento de software.

tons de pele, gerando principalmente classificações divergentes para a mesma expressão, além de apresentar uma classificação tendenciosa majoritariamente ao gênero masculino. A partir disso, pudemos instigar debates imediatos, permitindo compreender as limitações técnicas e os preconceitos sociais embutidos nos sistemas. As discussões produzidas a partir das falhas e vieses observados coletivamente demonstraram que a compreensão da problemática foi construída diante da expectativa dos resultados dos sistemas e seu desempenho real, o que foi identificado em entrevistas feitas com participantes da atividade, descritas abaixo.

As imagens capturadas eram excluídas imediatamente no fim do processo, para garantir que nenhum dado pessoal fosse armazenado ou enviado a servidores de terceiros, uma preocupação que foi discutida na produção da instalação e foi mencionada algumas vezes por participantes do evento. Àqueles preocupados com a captura e o compartilhamento de suas fotos, foi explicado que o experimento foi desenvolvido de modo que o ambiente de execução não se comunicasse com servidores externos. Portanto, para além das discussões sobre as classificações estimadas pelos algoritmos, foi possível explicar o processo de comunicação entre servidores e as precauções tomadas pelo grupo na escolha do código e no desenvolvimento do formato do experimento. Posteriormente, na oficina “Passando a Visão: vieses e impactos do Reconhecimento Facial”, que será descrita mais adiante, foram apresentados os desafios técnicos e éticos do RF, instigando ainda mais a percepção crítica.

Vale ressaltar que houve alguns obstáculos durante o processo, como a necessidade de se traduzir alguns conceitos técnicos, a resistência inicial de algumas pessoas em expor o rosto diante da câmera, o tempo limitado para o aprofundamento de certos pontos da discussão e dificuldades técnicas, incluindo a iluminação do local e a instabilidade da detecção nos sistemas. Reconhecer esses limites se faz fundamental para situar os alcances e obstáculos do próprio processo extensionista.

Com isso, buscou-se não apenas apresentar o objeto de estudo do grupo de extensão, mas também fomentar uma reflexão coletiva sobre seus impactos sociais e políticos. Essa reflexão foi construída a partir da experimentação realizada pelos próprios participantes, isso inclui os erros de detecção e as classificações incoerentes, os quais promoviam questionamentos imediatos quanto ao funcionamento dos sistemas, evidenciando a dicotomia sobre quem é mais facilmente reconhecido ou mais frequentemente mal interpretado por eles. As discussões

conduzidas durante a instalação e experimentação permitiram relacionar as falhas e vieses reproduzidos na problemática da vigilância urbana e segurança pública, bem como o racismo algorítmico e a desigualdade no tratamento de dados. Assim, a criticidade não se deu apenas pela afirmação dos proponentes da ação extensionista, e sim da interação direta entre o grupo e as limitações concretas dos sistemas de reconhecimento facial utilizados, de maneira que a experimentação técnica se convertesse em debate público.

Como parte da coleta de dados das atividades citadas, Pietra Milani Bizerril realizou entrevistas breves de caráter semiestruturado, gravadas mediante consentimento, conduzidas logo após a experimentação de alguns participantes na instalação Bota a cara, a fim de compreender suas percepções sobre os erros e vieses dos sistemas de Reconhecimento Facial. A seleção dos entrevistados não se deu de forma probabilística, mas seguiu um critério intencional (purposive sampling) em que foram convidados a participar aqueles que, durante a oficina, demonstraram maior interesse, expressaram curiosidade sobre os resultados obtidos ou se aproximaram espontaneamente para conversar sobre sua experiência. Desse modo, a participação foi voluntária, e nem todos os participantes da oficina foram entrevistados. O objetivo dessas entrevistas foi compreender como os participantes percebiam os erros, ambiguidades e vieses dos sistemas de Reconhecimento Facial a partir da experimentação técnica envolvendo seus corpos. Entre os relatos coletados, destacou-se o depoimento de uma pessoa negra e não binária, cuja experiência evidenciou de forma contundente como esses sistemas reproduzem desigualdades e tendem a falhar de maneira mais recorrente diante de corpos que escapam das normatividades de raça e gênero presumidas pelos modelos algoritmos.

Fiquei curioso para saber como a tecnologia, que parâmetros ela tem para identificar o gênero das pessoas, para ter essa informação afirmativa sobre o gênero de alguém. E também fiquei curioso sobre as emoções, porque dependendo dos tipos de emoções, uma delas [classificada pelo algoritmo] da Microsoft, as emoções que a gente tem, ela [a Microsoft] reconhece gêneros diferentes e também ambas [Microsoft e Meta] reconhecem mais tristeza em pessoas negras, ou de quem tem traços mais marcados, assim, mais negroides; reconhecem mais tristezas e não reconhecem felicidade, diz que é uma emoção neutra. (Entrevistado 1, 2024).

Diante dos depoimentos coletados no evento, considera-se que a experimentação técnica com diferentes algoritmos de Reconhecimento Facial realizada na

Criptofunk produziu indícios qualitativos consistentes de que a atividade contribuiu para alcançar os objetivos de intervenção crítica propostos pelo projeto de extensão. As falas registradas revelaram que a atividade provocou questionamentos espontâneos sobre a precisão, os vieses e os impactos sociais desses sistemas, especialmente quando participantes observaram discrepâncias entre suas características percebidas e as classificações produzidas pelas máquinas. Esse movimento de problematização emergiu tanto nas reações imediatas aos resultados quanto nas interpretações posteriores compartilhadas nas entrevistas, indicando que a vivência prática abriu espaço para uma reflexão situada sobre a tecnologia.

No contexto de ações de ativação comunitária, em que o propósito central é estimular processos coletivos de consciência, debate e apropriação crítica, o engajamento verbalizado pelos participantes constitui um indicativo relevante dos efeitos da intervenção. Ao tornar perceptíveis, por meio da experiência corporal, as limitações e inconsistências do Reconhecimento Facial, a oficina favoreceu a formulação de leituras críticas por parte das pessoas presentes, ampliando o diálogo sobre os impactos dessas tecnologias para grupos que vivenciam com maior intensidade seus riscos e assimetrias.

Compreende-se que, a partir de uma proposta de experimentação técnica dialógica, na qual a atividade de extensão se torna um meio de se repensar as políticas urbanas junto às comunidades, é possível construir saberes sobre a tecnociência que agreguem conhecimentos e realidades diversas, democratizando o debate sobre como tais dispositivos podem afetar diferentes corpos. Esses saberes são o amálgama entre os aportes conceituais e técnicos sobre as dimensões institucionais e os riscos do Reconhecimento Facial trazidos pela equipe do presente projeto de extensão e o conhecimento prático, vivido, mas também conceitual – na condição de lente de interpretação dos fenômenos sociais – de participantes das oficinas e das experimentações. A construção de saberes foi constatada nas falas das pessoas entrevistadas por Pietra Milani, como o trecho a seguir. “Fiquei muito empolgada com o Bota a Cara. É muito interessante a forma em que expõe os erros e os acertos de um Reconhecimento Facial e traz muitas reflexões” (Entrevistada 2, 2024). Também foi impactado pelos relatos colhidos no evento, especificamente sobre a necessidade de reforçar que toda imagem ou informação gerada no Bota a Cara seria excluída imediatamente, de que a presença do Reconhecimento Facial é ora naturalizado (em portarias de prédios e academias, por exemplo), ora visto com desconfiança e preocupação.

“Passando a Visão”: vieses e impactos do Reconhecimento Facial

Esta atividade, realizada em parceria com a campanha nacional #TireMeuRostoDaSuaMira, foi dividida em apresentações de conceitos relacionados ao Reconhecimento Facial e uma etapa de discussão coletiva com os(as) participantes, que contribuíram com suas perspectivas sobre o RF.

Inicialmente foram abordados os desafios técnicos e éticos do Reconhecimento Facial. Relacionando com a experiência da instalação “Bota a cara”, Rodrigo Firmino, André Pecini e Rubia Sehnem apresentaram conceitos básicos sobre o funcionamento dos algoritmos de aprendizado de máquina e de visão computacional, desde seus componentes considerados técnicos (Hora, 2023) até as noções de vieses algorítmicos (Buolamwini, 2017; O’Neil, 2021) e racismo algorítmico (Silva, 2020). Em seguida, as limitações técnicas dessas tecnologias foram discutidas por Carolina Israel, como a questionável premissa de universalidade das expressões faciais assumida pelos dispositivos algorítmicos, bem como a necessidade de que essas expressões sejam interpretadas no contexto social onde ocorrem (Barrett, 2021). A tais limitações, acrescenta-se aquelas relacionadas à baixa representatividade racial dos bancos de imagens de faces usados para treinar os modelos algorítmicos, que acabam por reproduzir e automatizar vieses (Rhue, 2018).

Após essa introdução, os cerca de 20 participantes foram divididos em 4 grupos e analisaram casos reais veiculados na imprensa, como prisões injustas baseadas em erros algorítmicos e o monitoramento de emoções em escolas. Esta atividade foi feita com a distribuição de notícias sobre o uso do Reconhecimento Facial e do Reconhecimento de Emoções na gestão pública – desde o monitoramento dos alunos nas escolas do Paraná (Audi, 2023), passando pela obrigatoriedade da captura biométrica de torcedores nos estádios de futebol (CNN Brasil, 2024), até os casos recorrentes de prisão de inocentes, majoritariamente pessoas negras (Sampaio, 2022). Os grupos foram incumbidos de refletir sobre a notícia que receberam e relatar casos que conhecessem.

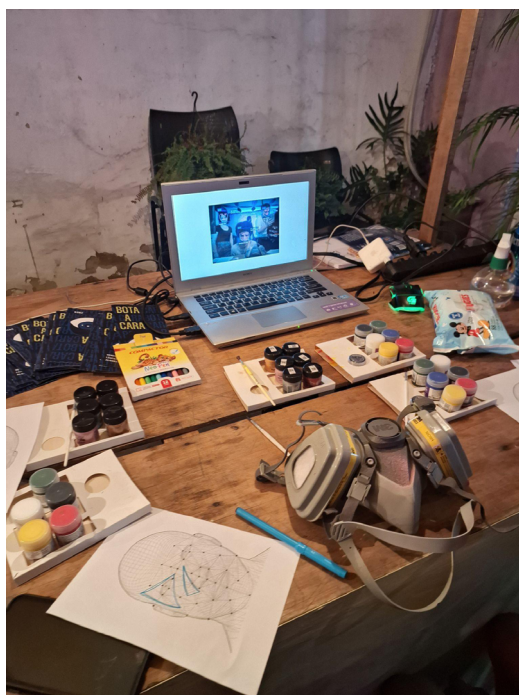
A oficina foi completada pelas exposições de Julia Abad sobre os problemas estruturais e questões éticas do RF e de Yasmin Rodrigues (O Panóptico) e Felipe Silva (Laboratório de Políticas Públicas e Internet – LAPIN) sobre racismo algorítmico. Além da apresentação do conceito de Tarcizio Silva (2022), foram discutidas formas de resistência a esses dispositivos de vigilância compostos por tecnologias, leis, acordos público-privados, lobbies, propaganda institucional etc. Entre as formas de resistência abordadas, destacam-se o letramento digital, que consiste

na habilidade de usar e compreender as tecnologias digitais de forma crítica, a regulamentação do Reconhecimento Facial na segurança pública e propostas de seu banimento, como a da campanha #TireMeuRostoDaSuaMira.

“Pinta a cara: quem vê cara não vê vigilância”

A oficina “Pinta a cara: quem vê cara não vê vigilância” visou promover uma experiência lúdica, criativa e crítica a partir de técnicas de maquiagem inspiradas em padrões antivigilância capazes de confundir sistemas de Reconhecimento Facial e de leitura automatizada de emoções. A atividade buscou articular a expressão artística com a reflexão sobre as implicações éticas, sociais e corporais das tecnologias de vigilância, evidenciando como o corpo pode se tornar, simultaneamente, alvo e instrumento de subversão frente ao vigilantismo facial biométrico.

Figura 2 – Instalação “Pinta a cara”. Material usado para a maquiagem e notebook com algoritmo de Reconhecimento de Emoções.



Fotografia: Pietra Milani/Acervo de projeto

A proposta partiu do entendimento de que os sistemas de RF operam com base na medição da distância entre pontos comuns do rosto humano, como olhos, boca, nariz, sobrancelhas e queixo, para confirmar identidades e estimar idade, gênero, raça e emoções. Tal funcionamento havia sido explorado previamente nas oficinas “Bota a cara” e “Passando a Visão”, que serviram como base conceitual para o entendimento do modo como os algoritmos “enxergam” os rostos humanos. Nessa oficina, contudo, o foco deslocou-se da observação do funcionamento da tecnologia para a experimentação de práticas que a contestam, demonstrando como a maquiagem pode distorcer a interpretação dos sistemas ao alterar e confundir o reconhecimento dos pontos de referência faciais.

Inspirada em estratégias artísticas e de ativismo digital, a oficina “Pinta a cara” ofereceu aos participantes a oportunidade de não apenas testar diferentes técnicas de maquiagem antivigilância, como também experimentar como os algoritmos de RF as interpretavam em comparação com a leitura facial que os mesmos realizavam dos seus rostos sem maquiagem. Os padrões utilizados foram inspirados no conceito de Computer Vision Dazzle (ou CV Dazzle), que aplica técnicas de maquiagem e penteados, planejadas com base no mapeamento de pontos de referência faciais, para criar assimetrias nos rostos, confundindo os sistemas automatizados (Harvey, 2011). Entre as estratégias abordadas estavam o uso de cores contrastantes em relação ao tom de pele, o ocultamento de traços marcantes como boca, olhos e ponta do nariz, além da aplicação de formas orgânicas e geométricas em direções incomuns. Ao alterar simetrias, destacar áreas específicas do rosto e ocultar outras, essas maquiagens fazem com que a máquina “não reconheça” ou interprete incorretamente identidades e emoções produzindo resultados diversos que puderam ser experimentados empiricamente pelos participantes.

Durante a atividade, observou-se que pequenas modificações, como a aplicação de linhas diagonais sobre a região dos olhos, o uso de cores contrastantes em torno da boca ou o ocultamento das sobrancelhas, foram suficientes para alterar significativamente as leituras dos algoritmos. Em alguns casos, os sistemas atribuíram gêneros diferentes aos mesmos rostos, identificando mulheres como homens e vice-versa, mas sempre definindo um gênero dentro do padrão binário pré-estabelecido. Esses casos foram especialmente significativos por evidenciar, de forma prática e visual, como o sistema de visão computacional depende da correspondência com um padrão normativo de rosto e como ele falha diante de expressões corporais e estéticas que escapam dessa padronização.

Outros participantes tiveram mudanças expressivas na estimativa de idade, sendo reconhecidos como muito mais jovens ou mais velhos do que nas experimentações sem maquiagem. As emoções variavam, às vezes sem parar, como se o algoritmo não conseguisse se decidir. Também houve situações mais raras em que os rostos deixaram de ser detectados completamente: o algoritmo não conseguia localizar os pontos de referência necessários para gerar o mapeamento, impedindo o funcionamento do Reconhecimento Facial.

A oficina gerou questionamentos sobre as possibilidades e limites dessas estratégias de resistência e de como as tecnologias rapidamente evoluem para superar essas lacunas. As experiências despertaram discussões espontâneas sobre a relação entre padronização algorítmica e diversidade dos corpos, especialmente em torno de como tecnologias de RF tendem a reforçar normas e estereótipos de gênero, idade e raça desconsiderando a multiplicidade de expressões, formas de existências e autodeterminação. O momento em que o algoritmo “errava” ou “falhava” foi interpretado não como um simples erro técnico, mas como um espaço de potência política e criativa, um gesto de desobediência algorítmica que permitia reimaginar o próprio ato de ser visto e identificado. Assim, a oficina “Pinta-a Cara” buscou mais que propor uma forma efetiva de burlar os sistemas de Reconhecimento Facial, mas estimular a expressão de formas estéticas de resistência e subversão por meio da combinação entre criatividade e reflexão crítica.

Live painting e arte como forma de resistência

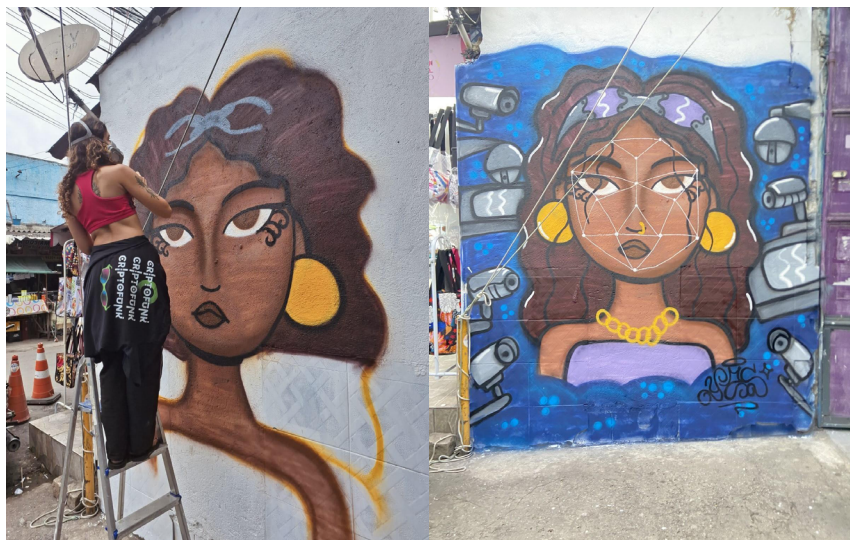
O *graffiti* é uma expressão artística e um dos pilares do movimento hip-hop, que ganha vida nos muros e em outras superfícies urbanas. Consiste na escrita de letras estilizadas que representam os vulgos (apelidos) dos artistas, além de personagens e outros desenhos com diferentes significados, feitos com tinta spray. Mais do que uma intervenção estética nas superfícies da cidade, o *graffiti* constitui uma prática de envolvimento e diálogo (Andron, 2023), funcionando como forma de expressão, ressignificação, subversão, voz e identidade, marcada pelas vivências dos sujeitos e por uma nova maneira de se relacionar o espaço urbano (Prosser, 2010).

Assim como o movimento do funk, o *graffiti* tem suas raízes na cultura periférica. Esses movimentos insurgentes e tecnopolíticos emergem das necessidades dos povos subalternizados de afirmar sua existência em meio à sociedade capitalista globalizada. Por meio desses atos culturais de resistência, expressão e lazer, esses movimentos emergem como ferramentas de transformação social, política

e cultural (Prosser, 2010). As culturas periféricas promovem empoderamento e pertencimento, atuando como táticas de incentivo à mudança (Roy, 2005).

Durante a Criptofunk, foi realizada uma performance de *live painting* pela escritora de *graffiti* YAS (Yasmin Marques). O mural abordava a temática da vigilância e do Reconhecimento Facial, uma das questões discutidas no evento, por meio da representação da personagem característica da grafiteira em interação com esses sistemas de controle.

Figura 3 – Produção do grafitti por YAS



Fotografias: Pietra Milani/Acervo de projeto

A intervenção realizada na área externa do galpão ressignificou o espaço, funcionando como uma ferramenta de comunicação entre as pessoas que circulavam pela região e as atividades internas, como oficinas e rodas de conversa. Por ser uma linguagem já presente e reconhecida naquele território, a intervenção foi acolhida pela comunidade, despertando curiosidade e questionamentos em crianças e adultos acerca do significado da pintura e do evento que estava acontecendo, convidando-os a entrar no espaço e se envolver com as atividades. Além de seu papel comunicativo, a ação assumiu um caráter lúdico, promovendo momentos de interação durante os intervalos da programação.

Um dos momentos marcantes durante a *live painting* envolveu uma criança de aproximadamente cinco anos, que demonstrou grande curiosidade pela imagem

representada no mural e pelo que ocorria no evento. Aos poucos, passou a participar das ações, enquanto recebia explicações sobre o tema e os objetivos da iniciativa, evidenciando compreensão e interesse.

CONSIDERAÇÕES FINAIS

Tecnologias de Reconhecimento Facial e de Expressões Faciais estão presentes nos mais diversos locais, das portarias de prédios e academias às salas de aula, onde impõem desafios a professores e professoras (Israel et. al, 2023). Seu uso na segurança pública é acompanhado por narrativas de eficiência e neutralidade, mas os casos de prisões de inocentes são o principal sintoma de que as câmeras inteligentes não funcionam isoladas dos processos tecnopolíticos dos quais participam. As atividades extensionistas descritas neste artigo proporcionaram mais do que a apresentação de seus elementos técnicos e de pesquisas acadêmicas sobre o tema. Promoveram a experimentação dos sistemas que produzem estimativas com base em traços biométricos, a discussão dos arranjos de vigilância e controle postos em funcionamento e de suas consequências para grupos sociais minorizados.

A experiência descrita neste artigo não apenas denunciou os riscos do Reconhecimento Facial na segurança pública, mas colocou em debate um reposicionamento da universidade e organizações da sociedade civil como agentes ativos na construção de saberes territorializados e dialógicos. Ao promover a experimentação técnica com algoritmos e oficinas participativas em um território como a Maré, o projeto rompe com a lógica tradicional da extensão verticalizada, promovendo trocas horizontais que integram conhecimentos acadêmicos, saberes populares e práticas culturais de resistência. Trata-se de uma partilha de experiências que não apenas informa, mas também transforma, tanto os participantes quanto os próprios pesquisadores e pesquisadoras envolvidos no processo.

As interações observadas ao longo das atividades indicaram um interesse significativo de participantes e visitantes ocasionais, que se engajaram espontaneamente nas demonstrações técnicas, nas discussões coletivas e nas práticas de criação propostas. Embora o evento não tenha contado com registro sistemático do número de participantes nem com instrumentos formais de avaliação qualitativa, as reações observadas – como expressões de surpresa diante das classificações algorítmicas, comentários críticos sobre racismo e gênero, e a permanência prolongada de algumas pessoas nas atividades – sugerem que as oficinas funcionaram como espaços importantes de provocação e reflexão.

A Criptofunk 2024 foi um espaço fundamental para ampliar o debate sobre tecnologia, vigilância e justiça social. O envolvimento da comunidade mostrou que, apesar da complexidade técnica dos algoritmos, suas consequências são sentidas de maneira concreta e cotidiana. A resistência tecnopolítica não passa apenas pela crítica, mas também pela criação de alternativas, ações educativas e formas de mobilização coletiva.

Nesse sentido, a ação na Criptofunk 2024 contribuiu para o fortalecimento de uma pedagogia tecnopolítica da extensão universitária na pós-graduação, em que o processo formativo se dá em meio ao conflito, à criatividade e à escuta atenta dos territórios periféricos. A pós-graduação deixa de ser exclusivamente um espaço de elaboração teórica e passa a operar também como um campo de intervenção sensível e situada, onde a produção de conhecimento se dá junto – e não apenas sobre – as comunidades impactadas pelas tecnologias de controle. A incorporação da cultura do funk, do *graffiti* e das performances de maquiagem como formas de investigação e intervenção reforça a importância de práticas extensionistas que reconheçam e valorizem a estética, a linguagem e as formas de resistência que emergem das margens.

Seis meses depois da oficina na Maré, o evento de lançamento do livro “O uso da Inteligência Artificial e a Inclusão Digital nos Serviços Públicos”, no Maravalley, Rio de Janeiro, uma das integrantes da mesa de debate discutia sobre os usos problemáticos do Reconhecimento Facial na segurança pública, quando uma participante da plateia mencionou o experimento da Criptofunk abordando o seu desconforto em ter seu gênero e idade definidos equivocadamente pelo software. Isso demonstra o impacto não só do experimento, mas de como as políticas de segurança também estão sendo observadas e questionadas pela comunidade.

Essa participação foi apenas a primeira de um total de quatro oficinas de ativação, previstas no projeto do PROEXT-PG até 2028, duas no Rio de Janeiro e duas em Curitiba. No entanto, ela proporcionou importantes reflexões acerca de como essas tecnologias reproduzem vieses e geram impactos significativos na vida das pessoas. É fundamental que projetos de extensão sigam promovendo ativações comunitárias, de maneira que as pessoas mais afetadas pelos vieses e violências tecnopolíticas tenham mais oportunidade de envolvimento crítico com o tema e desenvolvam autonomia frente ao impacto dessas tecnologias em suas vidas.

Ao articular pesquisa, arte, ativismo, formação universitária e a própria extensão como prática situada de engajamento público, a iniciativa narrada neste artigo inaugura modos possíveis de reconfigurar a relação entre universidade

e sociedade. Em um contexto de vigilância crescente e de aprofundamento das desigualdades digitais, a extensão crítica pode ser uma via fundamental para re-posicionar a universidade como aliada das lutas por justiça social e epistêmica. A Criptofunk não foi apenas um evento: foi um laboratório vivo de partilha e de produção de futuros, onde a crítica ao presente se combinou à criação coletiva de alternativas. Essa experiência revela o enorme potencial das práticas extensionistas para democratizar a produção de saber, fomentar a autonomia comunitária e reposicionar o papel da universidade na defesa de direitos.

AGRADECIMENTOS

Os autores agradecem à CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, pelo apoio financeiro ao projeto de extensão na pós-graduação que tornou possível a realização do presente artigo. O presente trabalho também contou com apoio do CNPq, Conselho Nacional de Desenvolvimento Científico e Tecnológico, e da Fundação Araucária.

Os autores agradecem ao data_labe por permitir a participação na programação da Criptofunk e à campanha #TireMeuRostoDaSuaMira pela parceria em uma das oficinas.

REFERÊNCIAS

ANDRON, S. *Urban surfaces, graffiti, and the right to the city*. London: Routledge, 2023.

AUDI, A. *Reconhecimento facial monitora emoções em escolas do Paraná*. Agência Pública, 27 out. 2023. Disponível em: <https://apublica.org/2023/10/reconhecimento-facial-no-parana-impoe-monitoramento-de-emocoes-em-escolas/>. Acesso em: 11/11/2025.

BARRETT, L. F. AI weighs in on debate about universal facial expressions. *Nature*, v. 589, n. 7841, p. 202–203, 2021.

Disponível em: <https://www.nature.com/articles/d41586-020-03509-5>. Acesso em: 20/05/2025.

BUOLAMWINI, J. A. *Gender shades: Intersectional phenotypic and demographic evaluation of face datasets and gender classifiers*. 2017. Dissertação (Mestrado em Artes e Ciências da Mídia) – Massachusetts Institute of Technology, Cambridge, 2017.

Disponível em: <https://dspace.mit.edu/handle/1721.1/114068>. Acesso em: 17/04/2025.

CASTIGLIONI, M. H. *[BR][Front-End] JavaScript – Reconhecimento Facial com FaceAPI*. 2020.

Disponível em: <https://youtu.be/aGecIY04ymQ?si=GzkYFxb5EvS7Kys0>. Acesso em: 16/05/2025

CNN BRASIL. *Reconhecimento facial será obrigatório nos estádios a partir de 2025*. CNN Brasil, 24 jul. 2024.

Disponível em: <https://www.cnnbrasil.com.br/esportes/futebol/reconhecimento-facial-sera-obrigatorio-nos-estadios-a-partir-de-2025/>. Acesso em: 11/11/2025.

CRIPTOFUNK. *Sobre*. [s.d.].

Disponível em: <https://criptofunk.com/>. Acesso em: 10/06/2025.

GOOGLE. *Guia de detecção de pontos de referência do rosto | Google AI Edge*. Google AI for Developers, [s.d.].

Disponível em: https://ai.google.dev/edge/mediapipe/solutions/vision/face_landmarker?hl=pt-br. Acesso em: 06/06/2025.

HAO, K. *A US government study confirms most face recognition systems are racist*. MIT Technology Review, 20 dez. 2019.

Disponível em: <https://www.technologyreview.com/2019/12/20/79/ai-face-recognition-racist-us-government-nist-study/>. Acesso em: 16/05/2025

HARVEY, A. *CV Dazzle*. Adam Harvey, 2011.

Disponível em: <https://adam.harvey.studio/cvdazzle/>. Acesso em: 14/06/2025 .

HORA, N. da. *MyNews explica! Algoritmos*. Coimbra: Edições 70, 2023.

ISRAEL, C. et al. *Reconhecimento Facial nas escolas públicas do Paraná*. Curitiba: Jararaca Lab, 2023.

Disponível em: https://jararacalab.org/cms/wp-content/uploads/2023/10/Relatorio_RF_2023.pdf. Acesso em: 02/05/2025.

MARQUES, I. C. Um breve relato sobre Inteligências Artificiais e os Estudos CTS. *CTS em foco*, v. 3, n. 2, 2023.

Disponível em: <https://esocite.org.br/images/BOLETIM-CTS/PDF/CTS-v3-n2.pdf>. Acesso em: 28/05/2025.

NUNES, P. et al. *Mapeando a vigilância biométrica*: Levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC, 2025.

Disponível em: https://drive.google.com/file/d/1bN2ssBp_dMiih8YOUnLhGL_5JRoNe5s/view. Acesso em: 10/06/2025.

O'NEIL, C. *Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia*. Santo André: Editora Rua do Sabão, 2021.

PANÓPTICO. *Monitor de novas tecnologias na segurança pública no Brasil*. 2025.

Disponível em: <https://www.opanoptico.com.br/#regioes>. Acesso em: 14/06/2025.

PASTOR, J. *Pintarte la cara de payaso es la forma perfecta de evitar el reconocimiento facial automático*. Xataka, 6 jul. 2018.

Disponível em: <https://www.xataka.com/robotica-e-ia/pintarte-cara-payaso-forma-perfecta-evitar-reconocimiento-facial-automatico>. Acesso em: 12/06/2025

PESCHANSKI, J. A.; JURNO, A. C.; HILSENBECK FILHO, A. M. Emergência da extensão universitária digital: boas práticas e direcionamentos. *Texto Livre*, v. 18, e56372, 2025.

PROSSER, E. S. *Grafite Curitiba*. Curitiba: Kairós, 2010.

REBELLO, A. *Smart Sampa*: Denunciada por corrupção irá capturar seu rosto em SP. Intercept Brasil, 14 ago. 2023.

Disponível em: <https://www.intercept.com.br/2023/08/14/smart-sampa-denunciada-por-corrupcao-capturar-seu-rosto-em-sp/>. Acesso em: 10/06/2025.

RHUE, L. *Racial Influence on Automated Perceptions of Emotions*. Rochester, NY: SSRN, 2018.

Disponível em: <https://papers.ssrn.com/abstract=3281765>. Acesso em: 12/11/2025.

ROY, A. Urban informality: Toward an epistemology of planning. *Journal of the American Planning Association*, v. 71, n. 2, p. 147-158, 2005.

SAMPAIO, F. *80% das prisões errôneas por reconhecimento facial no RJ são de negros*. Radioagência Nacional, 12 jan. 2022.

Disponível em: <https://agenciabrasil.ebc.com.br/radioagencia-nacional/justica/audio/2022-01/80-das-prisoas-erroneas-por-reconhecimento-facial-no-rj-sao-de-negros>. Acesso em: 09/11/2025.

SCHIFFLER, V. R. *Criando Detecção Facial com JavaScript e Face-api.js*. 2021.

Disponível em: <https://youtu.be/tF36BEoQcyo?si=M38tM6WLZeufSsWa>. Acesso em: 12/11/2025

SILVA, T. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. São Paulo: Edições Sesc SP, 2022.

TAIGMAN, Y. et al. Deepface: Closing the gap to human-level performance in face verification. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2014. p. 1701–1708.

Disponível em: http://openaccess.thecvf.com/content_cvpr_2014/html/Taigman_DeepFace_Closing_the_2014_CVPR_paper.html. Acesso em: 09/06/2025.

♦ VOL. 14, 2026, ISSN:2318-2326. PUBLICAÇÃO CONTÍNUA.

Todos os textos publicados na Interfaces – Revista de Extensão da UFMG são regidos por licença Creative Commons CC By.

A Interfaces convida pesquisadoras e pesquisadores envolvidos em pesquisas, projetos e ações extensionistas a submeterem artigos e relatos de experiência para os próximos números.

Os textos deverão ser enviados através do nosso endereço na web. No site estão disponíveis as normas para publicação e outras informações sobre o projeto. Vale ressaltar que os autores poderão acompanhar todo o processo de submissão do material enviado através desse site e que o recebimento de submissões possui fluxo contínuo.

www.ufmg.br/revistainterfaces

Contato: revistainterfaces@proex.ufmg.br

