Andreia Machado Oliveira, Felix Rebolledo Palazuelos *

AI Art de olho na vigilância da IA

*

Andreia Machado Oliveira é artista pesquisadora em arte, ciência e tecnologia. Pesquisadora do CNPq, da FAPERGS e Pesquisadora Associada da WITS University/África do Sul. Pós-doutora na School of Creative Media, na City University of Hong Kong. Doutora pela Universidade Federal do Rio Grande do Sul, com estágio doutoral na Université de Montreal, com pesquisa em Arte e Tecnologia. Docente do Departamento e Programa de Pós-graduação em Artes Visuais/UFSM. Vice-diretora do Centro de Artes e Letras – CAL/UFSM. Coordenadora do LabInter (https://www.ufsm. br/laboratorios/labinter) e líder do gpc.interArtec/CNPq.
<andreiaoliveira.br@gmail.com>
ORCID 0000-0002-8582-4441

Felix Rebolledo Palazuelos é pós-doutor em Estudos da Comunicação pela Universidade Federal de Santa Maria (UFSM), RS, Brasil. Doutor em Psicologia Social e Institucional pela Universidade Federal do Rio Grande do Sul

Resumo Esta investigação explora como o campo da *AI Art* tem se voltado para questões de vigilância que fazem uso de inteligência artificial. Essas tecnologias de vigilância, que utilizam visão computacional de última geração, como rastreamento ocular, e decisões algorítmicas avançadas, impactam significativamente quanto à privacidade e o controle de subjetividades. Examinamos como alguns artistas criticam as questões de vigilância em suas propostas artísticas, nos falando sobre uma vigilância ao mesmo tempo velada e declarada. Ainda, problematizamos tais questões de uma maneira muito particular no trabalho CyberFaces (2023), do LabInter/Brasil. Ao destacar a natureza invasiva da vigilância, nosso estudo enfatiza o papel da arte na formação de uma compreensão reflexiva e abertura para discussões sobre vigilância na sociedade contemporânea. Portanto, de forma crítica, este artigo nos leva a pensar nos sistemas operacionais e no funcionamento das tecnologias de IA, nos seus sistemas de armazenamento e compartilhamento e na dinâmica ambígua de uma vigilância da IA desejada e explícita, e, muitas vezes concomitantemente, rejeitada e negada.[1]

Palavras-chave *AI Art*, Vigilância, Inteligência Artificial, Arte Computacional.

(UFRGS), Porto Alegre, RS, Brasil. Mestre Fine Arts and Bachelor in Fine Arts com Habilitação em Cinema Production pela Concordia University, Montreal, Canadá. Bacharel em Engenharia Civil pela University of New Brunswick, Fredericton, Canadá. Membro do LabInter (https://www.ufsm. br/laboratorios/labinter).

<rebfel@gmail.com>

ORCID 0000-0002-7058-9637

AI Art's watchful eye on AI surveillance

Abstract *This investigation explores how the field of AI Art has turned to surveillance issues that make use of artificial intelligence. These surveillance technologies, which use computer vision, such as eye tracking, and advanced algorithmic decisions, have a significant impact on the privacy and control of subjectivities. We examine how artists criticize issues of surveillance in their artistic proposals, telling us about a surveillance that is both veiled and declared. Furthermore, we problematize such issues in a very particular way in the artwork CyberFaces (2023), by LabInter/Brazil. By highlighting the invasive nature of surveillance, our study emphasizes the role of art in forming a reflective understanding and openness to discussions about surveillance in contemporary society. Therefore, critically, this article leads us to think about operational systems and the functioning of AI technologies, their storage and sharing systems, and in the ambiguous dynamics of desired and explicit AI surveillance, and, often concomitantly, rejected and denied.*

Keywords *AI Art, Surveillance, Artificial Intelligence, Computer Art.*

AI Art con ojo en la vigilancia de la IA

Resumen *Esta investigación explora cómo el campo del AI Art se ha enfocado en cuestiones de vigilancia que hacen uso de inteligencia artificial. Estas tecnologías de vigilancia, que utilizan visión computacional de última generación, como el rastreo ocular y decisiones algorítmicas avanzadas, impactan significativamente en la privacidad y el control de subjetividades. Examinamos cómo artistas critican las cuestiones de vigilancia en sus propuestas artísticas, hablándonos sobre una vigilancia que es a la vez velada y declarada. Además, problematizamos tales cuestiones de una manera muy particular en el trabajo CyberFaces (2023) del LabInter/Brasil. Al destacar la naturaleza invasiva de la vigilancia, nuestro estudio enfatiza el papel del arte en la formación de una comprensión reflexiva y apertura para discusiones sobre vigilancia en la sociedad contemporánea. Por lo tanto, de manera crítica, este estudio nos lleva a pensar en los sistemas operativos y en el funcionamiento de las tecnologías de IA, en sus sistemas de almacenamiento y compartición y en la dinámica ambigua de la vigilancia de la IA, deseada y explícita y, a menudo al mismo tiempo, rechazada y negada.*

Palabras clave *AI Art, Vigilancia, Inteligencia artificial, Arte Computacional.*

Introdução

Sabemos que o grande olho que nos vigia atualmente passa pelos sistemas de inteligência artificial, nos monitorando constantemente, e na maioria das vezes veladamente, como o "grande olho de Deus que tudo vê". Neste sentido, este artigo explora como o campo da *AI Art* tem se voltado para questões de vigilância que fazem uso de inteligência artificial. Essas tecnologias de vigilância, que utilizam visão computacional de última geração, como rastreamento ocular, e decisões algorítmicas avançadas, impactam significativamente quanto à privacidade e o controle de subjetividades individuais e coletivas.

No campo da *AI Art*, examinamos como artistas como Trevor Paglen e Lauren Lee McCarthy criticam as questões de vigilância em suas propostas artísticas, nos falando sobre uma vigilância velada, e mesmo revelada e consentida. Ainda, problematizamos tais questões de uma maneira muito particular no trabalho CyberFaces (2023), produzido pelo Laboratório Interdisciplinar Interativo , vinculado ao Programa de Pós-graduação em Artes Visuais da Universidade Federal de Santa Maria (LabInter/PPGART/UFSM).

Ao destacar, desde sempre, a natureza invasiva da vigilância, nosso estudo enfatiza o papel da arte na formação de uma compreensão reflexiva e na abertura para discussões sobre vigilâncias constantes na sociedade contemporânea. Abordamos as decorrências sociais da vigilância no domínio da IA como base para uma investigação estética. Autores como Jeremy Bentham, Michel Foucault, Joanna Zylinska, Giselle Beiguelman, entre outros, têm explorado as implicações da vigilância da IA nas esferas sociais e políticas. Entendemos que tais implicações representam riscos significativos aos direitos individuais e coletivos, às ideais democráticas e à diversidade social.

Portanto, de forma crítica, este artigo nos leva a pensar nos sistemas operacionais e no funcionamento das tecnologias de IA, nos seus sistemas de armazenamento e compartilhamento e na dinâmica ambígua de uma vigilância velada e ao mesmo tempo explícita da IA. Esta ambiguidade faz parte do próprio controle implicado na vigilância, que ora teme e ora deseja ser notado e vigiado, que ora prima pelo cuidado e ora evita o próprio controle.

Vigilância e inteligência artificial

Na intersecção entre a inteligência artificial (IA) e a arte, a *AI Art*, nossa investigação se direciona para os usos e problematizações da IA na arte, na ciência e na tecnologia, com foco particular no nexo entre IA, vigilância e estética. É evidente e conhecido que várias práticas de vigilância baseadas em IA são atualmente utilizadas em todo o mundo, por governos, instituições militares, entidades empresariais de diversas origens e por interesses diversos. Também sabemos que práticas de vigilância sempre fo-

ram uma constante nas relações sociais e políticas, alternando e diversificando suas tecnologias, dependendo da época e do lugar. Ou seja, estarmos sob um sistema de vigilância não é algo novo com a IA, nem restrito a um sistema político e social específico. O que observamos são graus e nuanças diferenciadas, em geral atrelados a questões geopolíticas, econômicas e governamentais.

Neste contexto, notamos que tem ocorrido uma mudança profunda nas metodologias de vigilância, muitas vezes a fim de promover agendas de governança autocrática, suscitando preocupações sobre invasões aos direitos fundamentais de privacidade, minando a confiança pública e os princípios democráticos. Tais tecnologias que fazem uso da IA tornaram-se ferramentas omnipresentes que influenciam o delicado metaequilíbrio entre privacidade, segurança, controlo social e governança (FONTES; HOHMA; CORRIGAN; LÜTGE, 2022). Neste sentido, muitas práticas de vigilância tornam-se justificadas pelo seu caráter ambíguo, ficando duvidoso os limiares entre os seus usos e intenções. Portanto, sob o pretexto de apelos urgentes à segurança pública e ao reforço da segurança (SCHUILENBURG,2024), bem como de esforços aparentemente benignos, como a promoção da inovação para fins ambientais ou pesquisas medicinais e sanitárias, com o controle dos corpos, a gestão do tráfego (FONTES; HOHMA; CORRIGAN; LÜTGE, 2022) e a análise científica do comportamento (TURGEON, S.; LANOVAZ, 2020), nos encontramos diante aos dilemas da vigilância que oscilam entre segurança e controle, entre cuidado e domínio.

Ainda, paradoxalmente, estas tecnologias, que incluem reconhecimento facial, detecção de objetos, análise comportamental, policiamento preditivo, identificação biométrica e sistemas de vigilância autónomos, muitas vezes operam de forma imperceptível, sem serem atravessadas por preocupações de transparência e responsabilização (BUOLAMWINI; GEBRU, 2018), principalmente por parte das *BIG Techs* que pretensamente querem se passar por neutras e isentas de responsabilidade.

O uso generalizado da vigilância para controlo social e a aplicação contemporânea da IA, através do cooptação de grandes volumes de dados, incutiram um sentimento de apreensão relativamente à liberdade nos espaços públicos e controle excessivo à subjetividade humana e a privacidade pessoal com dinâmicas de poder e as implicações do monitoramento onipresente e seus efeitos sobre o psicológico. O uso contínuo de práticas tradicionais de vigilância e sua evolução híbrida para o domínio digital foram extensivamente analisados por estudiosos como Foucault (1987), Zuboff (2019), Lyon (2018) e Marx (1989, 2016), entre outros. Essas práticas, agora integradas e intensificadas por meio de tecnologias como *Deep Learning*, são significativamente aumentadas e intensificadas pela dinâmica de poder, aprimorada e possibilitada pela IA (SCHUILENBURG, 2024) e pelo processo generalizado de dataficação (FONTES; HOHMA; CORRIGAN; LÜTGE, 2022). Este hibridismo complexo permite-nos descrever a natureza generalizada da vigilância da IA atual como o "Panopticon 2.0" (ATES, 2021), que é notavelmente eficaz no controlo comportamental e na manipulação psicológica

de grupos sociais, refletindo uma transformação substancial no âmbito social e nas capacidades da vigilância e seus mecanismos.

Vigilância e o panopticon

A dinâmica tecnológica da vigilância velada da IA tem suas origens no conceito do panopticon do filósofo e jurista inglês Jeremy Bentham (1748–1832), no qual a subjugação e a disciplina são internalizadas e incorporadas por uma população desavisada, como "um novo modo de obter poder da mente sobre a mente" (BENTHAM, 1995, p. 31, tradução nossa). Este poder sobre a mente estava atrelado ao poder sobre os corpos, via uma composição arquitetônica. "O *Panóptico* de Bentham é uma figura arquitetural dessa composição" (FOUCAULT, 1999, p. 165) cujo efeito surge da replicação tecnológica na Terra da relação "ficcional" de Deus com a humanidade (BENTHAM, 1995, p. 11). Conforme proposto por Bentham em 1787, o dispositivo consiste em um edifício circular para a vigilância de prisioneiros dentro de instituições penitenciárias, onde o centro é ocupado por uma estrutura de torre que serve como alojamento do inspetor e a circunferência consiste em celas de detenção para prisioneiros, dispostas de tal forma que ambos são separados por um espaço vazio chamado área intermediária ou anular (BENTHAM, 1995). Do ponto de vista da torre central de observação, o inspetor pode vigiar as atividades de todos os presos o tempo todo por trás de aberturas que permitem "ver sem ser visto" (BENTHAM, 1995). "Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar" (FOUCAULT, 1999, p. 166). Observamos que esta figura arquitetural se replica em diversas instancias institucionais de poder, aplicada a diversos corpos que "precisam" ser subjugados. Assim, "as pessoas a serem inspecionadas devem sempre se sentir como se estivessem sob inspeção" (BENTHAM, 1995, p. 43, tradução nossa): os presos assumiriam que estão sempre sendo observados e, portanto, regulam seu próprio comportamento (FOUCAULT, 1999).

O modelo penitenciário de Bentham serviu como protótipo para casas penitenciárias ao longo dos séculos XIX e XX, "nas quais os objetos de *custódia segura, confinamento, solidão, trabalho forçado* e *instrução*" (BENTHAM, 1995, p. 34, tradução nossa, grifo do autor) precisavam ser mantidos à vista. A noção do panopticon poderia ser aplicada a "*prisões perpétuas* [...], *casas penitenciárias*, ou *casas de correção*, ou *casas de trabalho*, ou *manufaturas* ou *manicômios*, ou *hospitais* ou *escolas*" (Idem.). Em seu livro *Vigiar e Punir: O Nascimento da Prisão* (1999), Foucault usou o Panopticon como o análogo que melhor descreve as instituições disciplinares e seus sistemas pervasivos de vigilância e controle. Segundo Foucault, o principal efeito do Panopticon é "induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder" (FOUCAULT, 1999, p. 166). Como nunca se sabe quando estão sendo vigiados, se sentem vigiados constantemente.

Trazendo a ideia de Panopticon para a realidade atual pós-digital, acreditamos que o dispositivo panóptico é completamente funcional em todas as esferas das experiências analógicas e digitais, nas quais qualquer aspecto de uso gera dados que podam ser detectados ou capturados, ou em que há interesse em como e por que a subjetividade é exercida pelo usuário. Demeterio e Parreno (2021) identificam três modos de vigilância digital capitalista: vigilância digital de mídia social, vigilância digital de comércio eletrônico e vigilância digital no local de trabalho, e em todos os três aspectos podemos discernir o panopticon em ação. A vigilância mais insidiosa acontece quando qualquer uso de dispositivos digitais é, de alguma forma, monitorado, observado, rastreado, registrado, armazenado, datificado, compilado, agregado, analisado, perfilado, compartilhado, vendido, explorado e monetizado.

À primeira vista, dada a compreensão popular das redes sociais digitais como relações reticulares de usuário para usuário, a ausência de uma presença supervisora óbvia dentro da estrutura relacional da rede social não pareceria conformar-se à figura arquitetônica panóptica. Em vez disso, os usuários individuais estão radialmente conectados à entidade corporativa que atua como um hub central panóptico, que desempenha as funções de porteiro, moderador, curador, acelerador, regulador, bússola moral e comutador de roteamento de conteúdo (PALAZUELOS, 2023). Esta estrutura radial cria um sistema de controle centralizado onde todos os usuários estão subordinados ao hub, com todas as comunicações passando por ele sob sua supervisão panóptica, assegurando visibilidade permanente. A rede social como observador onipotente e onisciente modula, modera e intermedia todas as interações, institucionalizando assim a estrutura relacional como uma arquitetura panóptica (Idem).

Ao navegar na internet ou usar redes sociais, muitos dos usuários se auto restringem ou se autocensuram por medo de punição ou retaliação (MARTIN, 2022; 2013). Eles se abstêm de comportamentos ou discursos que possam ser considerados impróprios porque sentem/sabem que estão sob constante observação pelo motor de busca ou plataforma, seja através dos algoritmos de moderação de IA que vigiam todas as comunicações e tráfegos nas redes digitais, seja por moderadores humanos reais, supervisores ou censores em sua rede, cuja função é adjudicar sobre intenções suspeitas, interesses ou conteúdos fora do centro. Se o monitoramento está realmente ocorrendo é irrelevante: como resultado de um medo internalizado de ação disciplinar ou represálias punitivas de autoridades indeterminadas, os usuários se autocensuram em sua expressão, limitam sua curiosidade e restringem sua navegação distraída.

Mas, como Bentham poderia perguntar nas circunstâncias atuais de vigilância encoberta e integração da IA para criar as condições para o Panopticon 2.0, "*quis custodiet ipsos custodes?*" — quem vigia os vigilantes? Será que este pode ser um dos papéis que a IA é chamada a desempenhar?

O Panopticon 2.0 da IA

No contexto da IA e da vigilância, o conceito Panopticon 2.0 não é apenas uma metáfora, mas uma realidade incorporada por uma panóplia de tecnologias. Estas tecnologias, muitas vezes operando de forma invisível, criam uma sensação de observação e controlo perpétuos muito além dos limites de qualquer estrutura física. Ou mesmo operando de forma visível, como a conhecida frase "você está sendo filmado", restringe qualquer forma de escolha entre ser vigiado ou não. Por exemplo, o uso generalizado de reconhecimento facial em espaços públicos através do uso de câmeras de vigilância exemplifica como as ferramentas de vigilância atuais internalizaram e automatizaram princípios panópticos, tornando a vigilância onipresente, porém discreta.

Contudo, mesmo identificando aspectos do panóptico na atualidade, não podemos dizer que vivemos guiados pelos mesmos princípios, uma vez que a vigilância pós-digital propõe sentimentos ambíguos de querermos ou não sermos vistos. Para Giselle Beiguelman já estamos em outo paradigma de vigilância:

> Dessa forma, a lógica da vigilância passa a operar segundo um novo paradigma. A ameaça não é mais a de sermos capturados por um olho onipresente do tipo Big Brother. Mas o reverso, o medo de não sermos visíveis e desaparecermos (BEIGUELMAN, 2021, p. 64).

Observamos que os sistemas de vigilância vigentes induzem que os usuários "voluntariamente" postem seus dados, compartilhem suas rotinas cotidianas e, mais ainda, recebam likes e interações constantemente. Assim, "todos controlam todos, a partir das interações pessoais, e o rastreamento passa a depender da extroversão da intimidade pessoal do sujeito em rede" (BEIGUELMAN, 2021, p. 65).

Além disso, é importante reconhecer que nenhuma tecnologia de vigilância atua como um precursor universal da vigilância por IA. Em vez disso, cada modalidade tem as suas raízes em tecnologias analógicas ou pré-digitais distintas que requerem operação e interpretação humana direta. Por exemplo, sistemas baseados em IA, como reconhecimento facial, detecção de objetos e análise comportamental, são construídos sobre os fundamentos de práticas de vigilância presencial, fotografia analógica, monitoramento de circuito fechado de televisão, psicologia comportamental, técnicas de policiamento e primeiros sistemas biométricos, como impressões digitais e fotos policiais. Agora, "você está sendo filmado" está dentro dos circuitos dos computadores em cada aceite e permissão que damos a fim de usarmos os *softwares* e plataformas.

Da mesma forma, as práticas de monitorização das redes sociais e da utilização da internet, da escuta clandestina e da intercepção de conversas e mensagens telefónicas, que hoje representam desafios à privacidade e às liberdades civis, evoluíram a partir de técnicas anteriores, como escu-

tas telefónicas, gravação analógica, monitorização de telecomunicações e grandes bancos de dados baseados em papel em grande escala (MAGUIRE; FROIS; ZURAWSKI, 2014).

A evolução destas tecnologias aperfeiçoou a nossa compreensão conceptual do que constitui a vigilância e dos seus objetivos, e alargou as suas aplicações e resultados. Os avanços tecnológicos e o aumento exponencial do poder computacional dotaram os sistemas de vigilância de IA com capacidades aprimoradas. Isso inclui maior automação, integração perfeita entre várias plataformas e dispositivos, processamento de dados em tempo real e a capacidade de analisar rapidamente conjuntos de dados massivos para extrair padrões repetidos e discernir estruturas ocultas nos dados.

Tais avanços representam uma transformação significativa nas tecnologias de vigilância, marcando uma mudança de um monitoramento prático e presencial para sistemas complexos e automatizados – e muitas vezes autônomos – que integram velhos e novos paradigmas tecnológicos nos sistemas complexos de vigilância dos dias atuais.

Estes outros modelos de vigilância recaem "na relação *entre* os indivíduos, em detrimento do controle centralizado sobre todos do panóptico do jurista inglês Jeremy Bentham (1748-1832)". (BEIGUELMAN, 2021, p. 64). A vigilância ocorre de maneira consentida, seja pela necessidade de navegar na web e concordar com as notificações e *cookies*, seja por concordar com o padrão de vigiar e ser vigiado, seja pelo desejo de ser visto e exposto intensamente.

Arte, IA e vigilância

A arte faz uma crítica poderosa à natureza generalizada da vigilância, enfatizando questões éticas relacionadas ao uso abusivo da tecnologia e à violação da privacidade e dos direitos pessoais. Tais questões muitas vezes são evidenciadas através de experiências estéticas interativas e lúdicas em propostas artísticas que tornam os aspectos intrusivos da vigilância tangíveis para o público. Além disso, os artistas exploram a relação dinâmica entre humanos e máquinas, mostrando como a IA afeta o comportamento e as interações, podendo ser através de artes performáticas, web artes, instalações imersivas ou interativas etc. que despertam curiosidades, reflexões e imaginações.

Dado um mundo onde a Inteligência Artificial está ligada ao Big Data e à Aprendizagem Profunda (*Deep Learning*), a fim de analisar, interpretar e codificar todos os aspectos da existência humana e não humana, a vigilância da IA serve como uma fonte incomensurável para a investigação crítica estética, a reflexão ética e a expressão criativa. Através de produções em *AI Art*, que incorporam tecnologias de vigilância, como visualização de dados e capacidade de resposta em tempo real em instalações interativas, os artistas provocam reflexões sobre questões de controle, a fim de desafiar à presença invasiva e velada dos sistemas de vigilância. A omnipresença de

sistemas automatizados de controlo melhora significativamente as capacidades de vigilância da IA alimentadas pelos dados gerados pela presença de sensores e sistemas de monitorização que traduzem a experiência humana e não humana em fluxos digitais de dados binários.

A visualização de dados é outra área crítica na qual os artistas tornam tangíveis conceitos abstratos como privacidade de dados, iniciando conversas sobre propriedade de dados pessoais, biológicos e direitos digitais. A arte, ao problematizar e especular, permite aos artistas projetar cenários futuros influenciados pelas tecnologias de vigilância, oferecendo visões distópicas ou utópicas que levam os espectadores a refletir criticamente sobre os futuros potenciais para os quais poderíamos estar caminhando, bem como para quais imaginários estamos nos abrindo.

Neste sentido, alguns artistas trabalham na direção de reivindicar ou subverter tecnologias de vigilância, habilitando comunidades para usos mais críticos. Ou na direção de criticar aqueles que estão no poder, integrando tecnologias e práticas artísticas de forma imprevista, a fim de desafiar usos e percepções. Ou ainda, encontramos propostas artísticas que se voltam para a documentação e arquivamento do desenvolvimento das tecnologias de vigilância, fornecendo registros que possibilitam compreensões inusitadas de como estas tecnologias foram integradas na sociedade e permaneceram de várias maneiras. Esta rica mistura de crítica, exploração e documentação sublinha o espaço dinâmico em que arte e tecnologia se cruzam na *AI Art*, questionando e redefinindo a vigilância e o determinismo computacional na vida contemporânea.

Seguindo esta direção, de forma crítica, os trabalhos do artista Trevor Paglen levam-nos a pensar nos sistemas operativos e no funcionamento das tecnologias de IA, nos seus sistemas de armazenamento e partilha, e na lógica de múltiplos conjuntos de formação de referência. Paglen destaca que existem "imagens invisíveis" às quais os humanos não têm acesso: imagens que pertencem a bancos de dados com um número insondável de imagens para humanos; imagens criadas internamente pelos próprios computadores para gerar uma solução; ou as imagens automáticas invisíveis do nosso subconsciente, capturadas em nossas vidas diárias sem que percebamos (OLIVEIRA, 2023). Falamos de um sistema de vigilância tão complexo que desconhecemos vários aspectos de seus mecanismos, sendo que "somos vistos (supervisionados) a partir daquilo que vemos (as imagens que produzimos e os lugares em que estamos)" (BEIGHELMAN, 2021, p. 63), mesmo que tenhamos consciência ou não de tal produção.

As propostas de Paglen provocam-nos a perguntar quem se beneficia com estas tecnologias e para que fins servem, sendo voltadas aos sistemas militares e políticos, às empresas, aos fins de marketing e publicidade etc. Paglen trata também da forma como as máquinas nos observam constantemente, de como estamos inseridos em bancos de dados e da estética da aglomeração de imagens geradas por inteligências artificiais de reconhecimento facial. Seu trabalho também tem uma relação muito forte com a privacidade, a vigilância e a coleta de dados, uma vez que podem promover

ou discriminar, aprovar ou rejeitar, tornar visível ou invisível, julgar ou fazer cumprir (OLIVEIRA, 2023). Faz-nos compreender que os sistemas de vigilância estão diretamente ligados aos sistemas de classificação social.

A artista americana Lauren Lee McCarthy também trata sobre vigilância na sua performance *LAUREN*, na qual ela se torna uma versão da assistente virtual Alexa da Amazon. McCarthy busca problematizar como somos vigiados constantemente. A artista almeja ser melhor do que a IA Alexa, instalando-se nas casas dos participantes por 24 horas para ajudá-los de qualquer maneira. Ambiciona aperfeiçoar a inteligência doméstica de Alexa (OLIVEIRA, 2023), uma vez que entende bem as demandas dos usuários.

> A artista explora a interação homem-máquina através das lentes do lúdico, da ironia e do pastiche, desmistificando as grandes promessas por trás de algumas IA, ao mesmo tempo em que levanta a questão da suspensão voluntária da privacidade – o que só começa a parecer estranho quando a espionagem é realizada por uma 'Alexa humana'. (ZYLINSKA, 2020, p. 133, tradução nossa).

McCarthy investiga como os processos ligados à IA podem ser compreendidos criticamente, demonstrando como podemos aceitar a conveniência cotidiana de uma IA em troca de uma perda de subjetividade, privacidade e dados pessoais, tendo uma tolerância passiva da vigilância doméstica (ZYLINSKA, 2020). "A cultura da vigilância está a tal ponto introjetada no nosso cotidiano que não nos intimida usar um vocabulário tão policialesco como "seguir" e "ser seguido" nas redes sociais" (BEIGUELMAN, 2021, p. 62).

De outra maneira, a proposta *CyberFaces*[2], desenvolvida pelo LabInter/PPGART/UFSM/Brasil, de autoria de Andreia Oliveira, Alisson Schmidt, Everton Santos, Leonardo Burmann e Matheus Moreno, é uma instalação interativa que, ao fazer uso da inteligência artificial para reconhecimento facial, problematiza questões de permissão de captura de imagens, identificação automática e privacidade pela vigilância por IA. Ao investigar as ramificações éticas do reconhecimento facial, desafia os interatores a considerarem as sutilezas do viés algorítmico, a partir das relações subjetivas que a IA propõe.

Usando uma webcam que reconhece rostos posicionados na frente da câmera, um código personalizado captura esses rostos como imagens para treinar a IA que, por sua vez, gera máscaras de mosaico que subvertem a identificação do reconhecimento facial. Junto com as máscaras digitais criadas sobre os rostos, diferentes frases se sobrepõem à (re)velação digital, como um comentário crítico do processo: frases amigáveis verdes, frases de atenção amarelas e frases de perigo vermelhas (Figura 1). Tais frases foram produzidas pela IA do ChatGPT intencionalmente, objetivando identificar padrões comportamentais em tais frases.

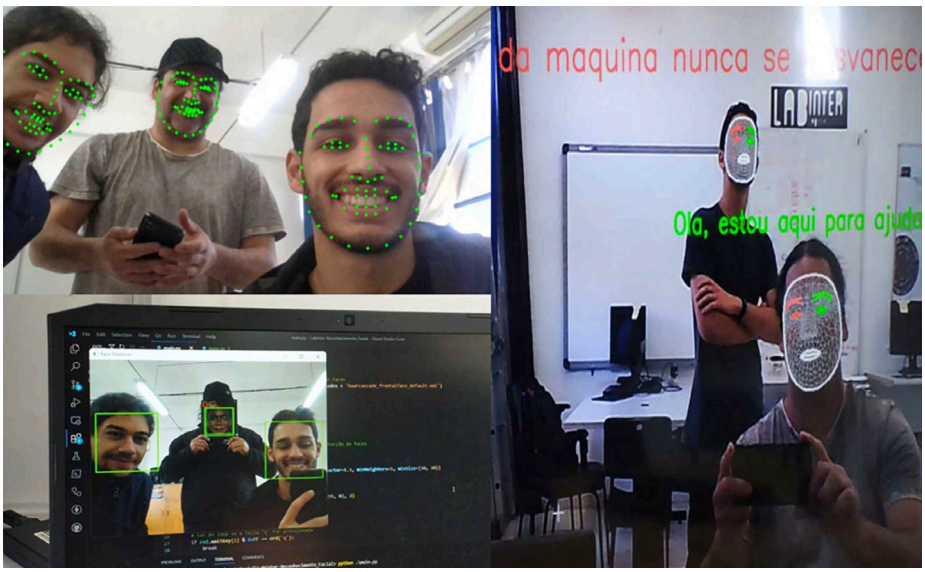

Figura 1. Estudos no LabInter para programação de *CyberFaces*.
Fonte: LabInter, 2024.

Há uma captura não apenas de rostos, mas um apagamento das diferenças entre os rostos, de suas singularidades e subjetividades, bem como uma homogeneização e sobrecodificação de preconceitos pré-programados que resultam das interações humano-máquina.

CyberFaces aguça conflitos como a permissão que o interator concede para a captura e armazenamento da imagem do seu rosto em troca de uma experiência lúdica e peculiar com a máquina e outros interatores. Ou mesmo o desejo de ver sua face exposta publicamente ao compor um mosaico de rostos (Figura 2), demonstrando o desejo de "estar sendo filmado" e a sua auto exposição consentida.

Figura 2. LabInter, *CyberFaces*, instalação interativa com IA, 2023. Apresentada na exposição de Matheus Moreno, 2024.
Fonte: LabInter, 2024.

Assim, *Cyberfaces* nos leva a pensar nas relações entre humanos e máquinas, nas maneiras que nos relacionamos com a IA considerando possibilidades amigáveis e de perigo, questionando as dinâmicas de vigilância

que nos são impostas (Figura 3). Também, leva-nos a perceber como as máquinas nos observam constantemente, como estamos inseridos em bancos de dados e em uma estética da aglomeração de imagens geradas por inteligências artificiais de reconhecimento facial. Propõem-nos um jogo de quem observa quem.

Figura 3. LabInter, CyberFaces, instalação interativa com IA, 2023. Apresentada na exposição de Matheus Moreno, 2024.
Fonte: LabInter, 2024.

Ao destacar a natureza invasiva da vigilância, nosso artigo enfatiza o papel da arte na formação de uma compreensão reflexiva e lúdica, e na abertura para discussões sobre os mecanismos da vigilância e sua presença omnipresente na sociedade contemporânea.

Algumas considerações

Portanto, percebemos que a arte pode desempenhar um papel crítico no desenvolvimento de contextos ético-políticos para a compreensão da vigilância da IA, de sua presença omnipresente e dos modos que tais vigilâncias se efetivam no momento atual. Ao problematizar a vigilância da IA em formatos diferenciados e interativos, a arte pode revelar implicações e repercussões da IA em nossas vidas. As propostas em *AI Art* que tratam da vigilância por IA servem como catalisadores para um discurso e diálogo, estimulando a consciência social e a partilha pessoal de experiências estéticas.

Propostas artísticas em uma perspectiva pós-digital, fazem uso da combinação de tecnologias analógicas e digitais, criando assim um terreno fértil para a exploração estética. Esta fusão não só expande as possibilidades artísticas, mas também abre novos caminhos para discussões sobre a relação entre tecnologia e sociedade, para articular a amplificação histórica e a sofisticação da tecnologia de vigilância, e para tornar visíveis as estratégias de vigilância de IA através da própria experiência de vigilância que a proposta artística propõe.

A partir de um princípio do panóptico, uma apreensão abstrata de que "alguém está ouvindo ou olhando" é suficiente para acionar a máquina de controle panóptico. De diferentes maneiras e circunstâncias, os usuários muitas vezes restringem seu uso porque temem que sua navegação desenfreada (consumindo sua produtividade), buscas intelectuais heterodoxas e curiosidades em geral, ou visões e comentários políticos não convencionais, resultem em repercussões punitivas ou intensificação da vigilância. Além disso, o medo da vigilância resulta não apenas da possibilidade de censura punitiva, mas do abuso percebido dos direitos pessoais e da dignidade decorrente da coleta de dados e invasão de privacidades resultantes de qualquer tipo de atividade sendo monitorada, coletada e relatada pelos inúmeros *cookies* e *spyware* que infestam nossos dispositivos digitais. O grau de auto restrição ou autocensura dependerá da conscientização dos usuários sobre qual atividade está sendo monitorada, na qual a vigilância está realmente ocorrendo e quais medidas disciplinares ou punitivas serão aplicadas às infrações.

Neste sentido, pensamos, aqui, as implicações sociais e subjetivas da vigilância no domínio da IA, como base para uma investigação estética, focando-se não apenas em uma análise crítica, mas também em uma sensibilização quanto as relações entre humanos e máquinas. Algumas criações poéticas que emanam das discussões sobre IA, visam infundir uma dimensão humanística, não excluindo o humano nas produções com IA. Como temos falado (OLIVEIRA, 2023; PALAZUELOS 2023), não há uma oposição entre humanos e máquinas, mas um agenciamento inerente que precisa ser questionado quanto a sua constituição. Não somos vigiados pelas máquinas, mas por humanos que estão agenciados com estas máquinas, pelo menos por enquanto. Ou melhor, "[...] os grandes olhos que nos monitoram veem pelos nossos olhos" (BEIGUELMAN, 2021, p. 63), ou seja, somos vigiados por máquinas que têm o olhar humano presente e oculto. Esse olhar do controle nos regula desde longa data, conforme Foucault coloca, mesmo antes da era clássica as técnicas de vigilância são minuciosas e se atém aos detalhes, uma vez que "todo detalhe é importante, pois aos olhos de Deus nenhuma imensidão é maior que um detalhe, e nada há tão pequeno que não seja querido por uma dessas vontades singulares" (FOUCAULT, 1999, p. 120). Assim, se pensarmos nos dias atuais, todos os dados são importantes, em cada dado fornecido há detalhes que falam de vontades singulares a serem rastreadas, classificadas, consideradas e predizíeis.

Como tal, propostas em *AI Art* incitam irmos além do uso passivo da IA em favor da promoção de uma compreensão das repercussões positivas e negativas da IA, com um foco crítico aos desdobramentos da vigilância da IA sobre nossos corpos e subjetividades, nossa vida cotidiana e desejos coletivos.

Notas

1. Apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul (FAPERGS).
2. Ver: https://www.ufsm.br/laboratorios/labinter/projetos/cyberfaces.

Referências

ATES, A. **The Evolution of Panoptic Surveillance and Its Impact on Political Discrimination**. IğdırÜniversitesiSosyalBilimlerDergisi, S.28, s. 202-216, 2021.

BENTHAM, J. **Panopticon or, The Inspection-house & C**. In The Panopticon Writings. (Ed. Božovič, M.). Verso, 1995.

BEIGUELMAN, Giselle. **Políticas da imagem: Vigilância e resistência na dadoesfera**. São Paulo: Ubu Editora, 2021.

BUOLAMWINI, J.; GEBRU, T. **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification**. Proceedings of Machine Learning Research 81:1–15, 2018.

DEMETERIO III, F. P. A. & PARRENO, J. B. **Meta critique on Bentham and Foucault's panoptic theories as analytic tools for threemodesof digital surveillance**. Plaridel. Advance online publication, 2021. Disponível: http:// www.plarideljournal.org/article/metacritique-on-bentham-and-foucaults-panoptic-theories-asanalytic-tools-for-three-modes-of-digital-surveillance/ Accesso: julho 20, 2024.

FONTES, C.; HOHMA, E.; CORRIGAN, C.; LÜTGE, C. **AI-powered public surveillance systems: why we (might) need them and how we want them**. Technology in Society Journal, 2022.

FOUCAULT, M. **Vigiar e Punir: Nascimento da prisão**. Petrópolis: Editora Vozes, 1999.

LYON, D. **The Culture of Surveillance**. Polity Press, 2018.

MAGUIRE, M; FROIS, C.; ZURAWSKI, N. **The Anthropology of Security: Perspectives from the Front line of Policing, Counter-Terrorism and Border Control**. Pluto Press, 2014.

MARTIN, C. D. **The Internet as a Reverse Panopticon**. ACM Inroads, 4(1), 8. doi:10.1145/2432596.2432599, 2013.

MARTIN, C. D. **The Internet as a Reverse Panopticon**. Computersand Society. Disponível em: https://computers-society.org/2022/03/10/the-internet-as-a-reverse-panopticon/. 2022. Acesso: julho 20, 2024.

MARX, G. T. **Undercover Police Surveillance in America**. Universityof California Press, 1989.

MARX, G. T. **Windows Into the Soul: Surveillance and Society in an Age of High Technology**. Universityof Chicago Press, 2016.

OLIVEIRA, A. M. **Future imaginings in art and artificial intelligence**. Journal of Aesthetics and Phenomenology, v. 9, n. 2, p. 209-225, 2023.

REBOLLEDO, F. P. **The Affective Toxicology of Social Media**. Revista FAMECOS, Porto Alegre, v. 30, p. 1 -17, jan.-dez. 2023 | e- 42648 DOI: https://doi.org/10.15448/19. Disponível:https://www.researchgate.net/publication/366937688_Affective_Toxicology_of_Social_Media. Acesso: julho 29 2024.

SCHUILENBURG, M. **Making Surveillance Public: Why you should be more woke about AI and Algorithms**. Eleven, 2024.

TURGEON, S.; LANOVAZ. **Tutorial: Applying Machine Learning in Behavioral Research**. PerspectBehavSci. 2020 Dec; 43(4): 697–723, 2020.

ZUBOFF, S. **The Age of Surveillance Capitalism: The Fight for a Human Future atthe New Frontier of Power**. Public Affairs Books, 2019.

ZYLINSKA, J. **AI Art, Machine Visions and Warped Dreams**. London: Open Humanities Press, 2020.

Recebido: 01 de agosto de 2024
Aprovado: 28 de setembro de 2024