EX±ACTO.
VI Congreso INTERNACIONAL DE INVESTIGACIÓN EN ARTES VISUALES
ANIAV 2024.
3-5 de julio 2024, Valencia
Doi: https://doi.org/10.4995/ANIAV2024.2024.17860

Estrategias de ofuscación. Prácticas artísticas para evitar ser reconocidas

Obfuscation strategies. Artistic practices to avoid being recognized

Claudia González
Universidad Complutense de Madrid, claugo16@ucm.es

Breve bio autora:

Licenciada en Bellas Artes (UCM, 2005), Máster en Investigación y Creación de Arte (UCM, 2010) y posteriormente MBA en Gestión de Empresas e Instituciones Culturales (Universidad de Salamanca, 2011). De manera profesional se dedica a la producción de proyectos artísticos y a la gestión cultural en torno al binomio arte y participación. Actualmente trabaja para el Ayuntamiento de Madrid en programas de descentralización y proximidad cultural en la ciudad. Como artista ha formado parte de varios colectivos y realizado exposiciones en espacios de Madrid como Off Limits, Sala de Arte Joven, Arquería de Nuevos Ministerios o ABM Confecciones y fuera de Madrid en el Festival Okuparte de Huesca o la Sala Alterarte de Ourense entre otros.

Como investigadora ha sido miembro del grupo de investigación de la Comunidad de Madrid En los márgenes del arte (ediciones 2018 y 2019). De 2017 a 2020 ha sido profesora colaboradora de la Facultad de Bellas Artes de la UCM y desde 2020 es investigadora predoctoral en esa misma institución. Su trabajo gira en torno a las prácticas estéticas con intencionalidad política; la esfera pública; y el arte y el activismo. Su tesis, en producción, versa sobre las "Prácticas estéticas de ocultación del rostro y su capacidad expansiva desde la web 2.0".

How to cite: González, C. (2024). Estrategias de ofuscación. Prácticas artísticas para evitar ser reconocidas. En libro de actas: *EX±ACTO. VI Congreso Internacional de investigación en artes visuales aniav 2024. Valencia*, 3-5 julio 2024. https://doi.org/10.4995/ANIAV2024.2024.17860

Resumen

Las tecnologías de reconocimiento facial tienen múltiples aplicaciones en controles fronterizos, análisis forenses, ciberseguridad y la vigilancia en general. También garantizan el acceso seguro a teléfonos, ordenadores y apps de pagos, nos permiten etiquetar a amigos en redes sociales y hasta diagnosticar enfermedades.

Sin embargo, la pérdida de privacidad a cambio de determinados servicios o en pos de una supuesta seguridad, conlleva algunos peligros. Existe una clara asimetría de poder entre los propietarios de las tecnologías y los que producimos los datos. Además del poco control que tenemos sobre el tratamiento y uso de nuestra información, debemos tener en cuenta que las tecnologías de la vigilancia operan enmarcadas en políticas de visibilidad repletas de sesgos de raza, género y clase.

En esta comunicación nos preguntamos sobre cuáles pueden ser las aportaciones del campo del arte a la hora de generar una visión crítica y otras posibilidades de acción frente a los sistemas de reconocimiento facial. Niessenbaum y Brunton definen "la ofuscación" como la adición deliberada de información ambigua, confusa o engañosa para interferir con la vigilancia y la recopilación de datos. Partiendo de este concepto, presentaremos una serie de propuestas artísticas en las que el uso del anonimato como estética experimental y forma política nos puede aportar un análisis transversal de algunas cuestiones complejas que implican la recopilación y tratamiento de nuestros datos. Máscaras de datos, maquillajes y cosméticos, o rostros prestados son algunas de las estrategias que los artistas proponen como defensas legítimas para evidenciar y paliar estas asimetrías. A través de estos casos veremos cómo el arte, desde una reflexión en ocasiones irónica,

en otras más comunitaria y pragmática, propone un imaginario de la invisibilidad y el anonimato que se constituye como una alternativa al hipercontrol en el que vivimos.

Palabras clave: *reconocimiento facial; políticas de la visibilidad; anonimato; máscara.*

Abstract

Facial recognition technologies have multiple applications in border controls, forensic analysis, cybersecurity and surveillance in general. They also guarantee secure access to phones, computers and payment apps, allow us to tag friends on social networks and even diagnose diseases.

However, the loss of privacy in exchange for certain services or in pursuit of supposed security, carries some dangers. There is a clear power asymmetry between the owners of the technologies and those of us who produce the data. In addition to the little control we have over the treatment and use of our information, we must take into account that surveillance technologies operate within visibility policies full of race, gender and class biases.

In this communication we ask ourselves what the contributions of the field of art can be when it comes to generating a critical vision and other possibilities of action regarding facial recognition systems. Niessenbaum and Brunton define "obfuscation" as the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection. Starting from this concept, we will present a series of artistic proposals in which the use of anonymity as an experimental aesthetic and political form can provide us with a transversal analysis of some complex issues that involve the collection and processing of our data. Data masks, makeup and cosmetics, or borrowed faces are some of the strategies that artists propose as legitimate defenses to highlight and alleviate these asymmetries. Through these cases we will see how art, from a reflection that is sometimes ironic, at other times more communal and pragmatic, proposes an imaginary of invisibility and anonymity that is constituted as an alternative to the hypercontrol in which we live.

Keywords: *facial recognition; visibility policies; anonymity; mask.*

1. INTRODUCCIÓN. ROSTROS BIOMÉTRICOS

Las anticipaciones de Deleuze sobre las sociedades de control (1999) o de Haraway sobre la informática de la dominación (1995) en los años 90 del siglo pasado nos hablaban de un sistema que nos observa, monitoriza y rastrea para producir datos sobre nuestros comportamientos y convertirnos en cifras. Hoy en día nuestros móviles, ordenadores y asistentes virtuales oyen nuestras conversaciones, recogen información sobre nuestras compras, nuestros planes de viajes y ocio y nuestros problemas de salud, comparten nuestras localizaciones en tiempo real y obtienen nuestras imágenes. Cotidianamente somos observad+s por satélites, vehículos que proporcionan las imágenes para los sistemas de navegación y por miles de cámaras de vigilancia instaladas en espacios públicos y privados. Vivimos el auge de los sistemas biométricos que permiten un reconocimiento automatizado de individuos en función de sus características biológicas y de comportamiento, como la huella dactilar, el rostro, el iris y la voz (Jain, Nandakumar y Ross, 2016, p. 80). "Medir el cuerpo se ha convertido en el fundamento de las políticas de seguridad globales" (Cruz y García, 2019, p. 29).

El rostro ha sido el sistema habitual empleado por las personas para reconocernos las unas a las otras, pero el trabajo para que este proceso fuera realizado por ordenadores empezó a mediados de 1960 por Woodrow W. Bledsoe y sus colegas de la Panoramic Research. Una larga evolución ha habido desde entonces hasta ahora, donde el reconocimiento facial se ha convertido en una de las formas preferidas para garantizar la seguridad de teléfonos, ordenadores y apps de pagos. También nos permite etiquetar a nuestr+s amig+s en redes sociales de forma fácil, e incluso acelerar el diagnóstico de determinadas enfermedades (Dolgin, 2019). Este tipo de sistemas tiene además múltiples aplicaciones en los controles fronterizos, análisis forenses, ciberseguridad y la vigilancia en general.

Una de las razones de que el reconocimiento facial sea uno de los sistemas biométricos más usados es la disponibilidad de grandes bases de datos recopiladas por autoridades y agencias gubernamentales de todo el mundo (Jain, Nandakumar y Ross, 2016, p. 82). Pero no sólo contamos con los registros oficiales, sino que con un rastreo de redes sociales se pueden encontrar prácticamente todas las caras que se necesiten. Otra ventaja con la que cuenta el reconocimiento facial frente a otros sistemas es la capacidad de capturar las imágenes de los rostros de forma encubierta (Jain, Nandakumar y Ross, 2016, p. 93). Las cámaras de vigilancia en el espacio público han proliferado considerándose un elemento disuasivo contra el crimen[1]. Y, gracias a los avances en el aprendizaje automático, capacidad de almacenamiento y potencia de procesamiento, los ordenadores han perfeccionado su método para hacer el reconocimiento facial más exacto a pesar de la edad, la posición o la iluminación.

Sin embargo, la pérdida de privacidad en pos de una supuesta seguridad o incluso al acceso a determinados servicios, tiene sus peligros. La recogida y tratamiento de la información se realiza a través de relaciones de poder asimétricas en las que nos encontramos en el lado débil. Rara vez tenemos la opción de elegir si somos monitoread+s o no, qué se hace con la información que se recopila o cómo nos repercuten las conclusiones extraídas de esa información (Brunton y Niessenbaum, 2015, p. 49). No sabemos qué tratamiento tienen esos datos en la actualidad y lo que quizás es más preocupante, no sabemos lo que los algoritmos, técnicas y bases de datos del futuro podrán hacer con nuestros datos. Un informe de la web abolishdatacrime.org desglosa las estrategias de criminalización de los datos (creación, archivo, robo y reventa) utilizadas para acechar a l+s inmigrantes y marcarl+s como amenazas por parte del Servicio de Inmigración y Control de Aduanas y el FBI en EEUU (Community Justice Exchange, 2022). Una investigación del Financial Times reveló que Microsoft había compartido públicamente una base de datos de 10 millones de imágenes de caras sin el conocimiento o consentimiento de los sujetos (Murgia, 2019). China utiliza la tecnología de reconocimiento facial para clasificar a las personas por etnia y cometer violaciones de los derechos humanos contra minorías étnicas como l+s uigures[2]. Además, uno de los problemas éticos más importantes en este tipo de tecnologías son los sesgos que contienen los conjuntos de muestras hacia los hombres blancos. Un informe de 2019 del Instituto Nacional de Estándares y Tecnología de U.S. (Grother, Ngan y Hanaoka, 2019) demuestra que existen dificultades en el reconocimiento facial dependiendo de la raza y el género. Los programas albergan mayor error de identificación en personas de raza asiática, afroamericana o nativos americanos frente a la raza caucásica y en mujeres frente a hombres, dando lugar a falsos positivos. Las consecuencias de este sesgo pueden incluir detenciones y acusaciones erróneas.

Además, debemos tener en cuenta los peligros que suponen la vulnerabilidad de la seguridad de las bases de datos y los sistemas biométricos que se pueden traducir en denegación de servicio a usuari+s legítimos, intrusión de usuari+s no autorizados, erosión de la privacidad y suplantación de identidad (Roberts, 2007).

Pero, ¿existen resquicios, grietas o debilidades en las industrias biométricas que pueden protegernos de esa relación asimétrica y hacer valer nuestra necesidad de privacidad en determinados momentos? ¿Hay alguna

[1] Se estima que hay más de 1 millón Cámaras CCTV sólo en la ciudad de Londres y alrededor de 4,9 millones de ellas están repartidas por todo el Reino Unido. (Barrett, 2013)

[2] Numerosos medios han publicado noticias a este respecto (Rollet, 2018), (Mozur, 2019).

manera de esquivar la vigilancia y la subsiguiente clasificación y estandarización de nuestros datos biométricos? ¿Nos podemos proteger de las políticas de vigilancia regidas de manera poco ética o de los abusos cometidos con nuestros registros faciales?

La legislación y las políticas de privacidad, las tecnologías de protección de datos como la criptografía, las acciones de divulgación y los códigos de prácticas profesionales son algunas de las respuestas a la hora de regular, o sortear el mal uso de nuestros datos por parte de determinadas corporaciones, anunciantes, industrias, gobiernos y otras partes interesadas.[3] Pero en esta comunicación queremos preguntarnos por las posibilidades que desde el arte, se han dado para plantear algunas alternativas a este sistema, tanto para burlarlo como para imaginar otras posibilidades de habitar o reflexionar de forma crítica sobre el mismo.

¿Cuáles pueden ser las aportaciones del campo del arte a la hora de generar una visión crítica y nuevas posibilidades de acción en los sistemas de reconocimiento facial?

2. METODOLOGÍA: ESTRATEGIAS DE OFUSCACIÓN. CONFUNDIR, ENGAÑAR E INTERFERIR

Niessenbaum y Brunton desarrollan en 2015 el concepto de "ofuscación" definiéndolo como "la adición deliberada de información ambigua, confusa o engañosa para interferir con la vigilancia y la recopilación de datos" (2015, p. 1). Esta idea aparentemente sencilla puede desplegarse en un amplio repertorio de prácticas y métodos para la desaparición, la pérdida de tiempo, el análisis frustrante, la desobediencia traviesa, la protesta colectiva y la reparación individual, entre otros.

En el campo del arte, las tecnologías de vigilancia han sido tratadas y problematizadas desde sus comienzos con la instalación de las primeras cámaras en los espacios públicos. Elke Reinhuber (2024), en un artículo recientemente publicado en Artnodes, traza un panorama de las formas en que l+s artistas han abordado el problema de la vigilancia en su trabajo en los últimos cincuenta años tanto para aumentar la concienciación sobre el mismo como para evadirlo. Numerosos proyectos comisariales y exposiciones internacionales también se han ocupado de este tema.[4]

Partiendo de la ofuscación como objetivo principal, y explorando la producción artística reciente, nuestro método de investigación consistirá en localizar y analizar una serie de casos desarrollados por artistas para hackear, hacer frente o dar la vuelta a los sistemas de vigilancia y control basados en las industrias biométricas y más específicamente en las tecnologías de reconocimiento facial. A partir del estudio de los ejemplos mencionados, veremos que el uso del anonimato como estética experimental y forma política es uno de los métodos más empleados por l+s artistas y nos puede aportar un análisis transversal de algunas cuestiones complejas que implican la recopilación y tratamiento de nuestros datos. Este análisis nos servirá para determinar las posibilidades que residen en un cierto arte crítico para proporcionar una contranarrativa que nos permita escapar de estos sistemas o por lo menos, contrarrestar su lógica de clasificación y estandarización de la información.

[3] En este sentido es interesante consultar la carta al Gobierno de España que escribe el Colectivo de investigación militante Bikolabs y que firman más de 70 academic+s y profesionales, solicitando una moratoria para estudiar el uso y comercialización de sistemas de reconocimiento y análisis facial por parte de empresas públicas y privadas y cuál debe ser la legislación europea al respecto (Bikolabs, 2021).

[4] La muestra "CTRL [SPACE] Rhetorics of Surveillance from Bentham to Big Brother" que tuvo lugar en el Zentrum für Kunst und Medientechnologie (ZKM) de Karlsruhe entre octubre de 2001 y febrero de 2002 explora una amplia gama de prácticas para investigar el estado del arte panóptico que implica la omnipresencia de la vigilancia en nuestra vida diaria a comienzos del siglo XXI. "Exposed: Voyeurism, Surveillance, and the Camera since 1870" organizada por la Tate Modern y el Museum of Modern Art de San Francisco en 2010 investiga cómo la cámara ha ido transformando el acto de mirar. "Faceless. Re-inventing privacy through subversive media strategies" exhibida en 2014 en el espacio de arte Mediamatic de Ámsterdam explora las consecuencias de la pérdida de privacidad como resultado del 11 de septiembre produciendo a su vez un aumento del interés de determinadas propuestas por el anonimato.

3. PROPUESTAS ARTÍSTICAS DISIDENTES

3.1. Máscaras en lugar de rostros

La propuesta de algun+s artistas pasa por crear máscaras que, superpuestas al rostro, confundan a los sistemas de reconocimiento facial. Utilizando estos propios sistemas y jugando con los datos proporcionados a los mismos, crean rostros amorfos que pueden ser utilizados como armas de defensa para luchar contra los sesgos y las clasificaciones algorítmicas o incluso para enfrentarse con sus propias formas de conocimiento del rostro humano.

El artista Sterlin Crispin en su proyecto "Data Masks" (2013-2015), crea una serie de máscaras usando los algoritmos de reconocimiento facial de manera inversa para revelar cómo estas tecnologías representan la identidad humana. Crispin entiende la tecnología como un súper-organismo global viviente formado por todas las máquinas y software, lo que él llama "el otro tecnológico" (2014, p. iv). La intención del artista es dotar de materialidad a la imagen que la tecnología tiene de lo humano, mostrando lo irreconciliable de los datos biométricos con la carne de los rostros de las personas.

Para Crispin, hacer visible lo digital se configura como un acto de protesta política que revela los mecanismos que subyacen tras el agresivo crecimiento de las técnicas de vigilancia y biometría usadas hoy (2014, p. 2). Según el artista, el objetivo de crear estas máscaras no es anular el reconocimiento facial o proporcionar algo indetectable, sino mostrarle a la máquina lo que está buscando, sostener un espejo frente al ojo que todo lo ve del panóptico digital en el que vivimos y dejar que mire dentro de su propia mente (2014, p. v). Las máscaras de datos desarrollan patrones que la tecnología identifica como rostros humanos, como una especie de pareidolia para los sistemas de visión por ordenador (2014, p. 13).

Fig. 1. *Data-Mask. Vista de la instalación en ZKM Karlsruhe. Septiembre de 2015. Cortesía del artista.*

El artista Zach Blas reflexiona sobre cómo detectó un aumento simultáneo de protestas enmascaradas junto con el auge de las industrias biométricas (Lee-Morrison, 2019, p. 142). A través de su obra, Blas propone una crítica a las tecnologías de reconocimiento facial entendiendo éstas como un brazo extendido de las estrategias políticas neoliberales que impactan de manera desigual a los grupos ya vulnerables y marginados de la sociedad. Lo que él argumenta es que el reconocimiento biométrico involucra un proceso computacional de estandarización con conjuntos de parámetros producidos a través de los sesgos inherentes a una historia de discriminación social. Este proceso computacional, explica Blas, tiene profundamente incrustado dentro de él una visualidad extraída de las normas sociales de género, raza y sexualidad (Lee-Morrison, 2019, p. 142).

El proyecto de Blas *Facial Weaponization Suite* protesta contra el reconocimiento facial biométrico, y las desigualdades que propagan estas tecnologías. Para ello el artista fabrica "máscaras colectivas" en talleres que se modelan a partir de los datos faciales agregados de l+s participantes, lo que da como resultado máscaras amorfas que no se pueden detectar como rostros humanos mediante el reconocimiento facial biométrico.

La primera máscara creada por Zack Blas es bautizada por el artista como *Fag Mask.* Es el resultado obtenido a partir de los datos faciales biométricos de los rostros de muchos hombres queer como respuesta a estudios científicos que relacionan la determinación de la orientación sexual a través de técnicas de reconocimiento facial rápido.

***Fig. 2**. Zach Blas, Fag Face Mask. 20 de octubre de 2012. Los Angeles, CA, de Facial Weaponization Suite 2012*
Tereftalato de polietileno reciclado, pintado y formado al vacío. Cortesía del artista.

El artista también ha creado máscaras que exploran las concepciones negativas de la negritud, el feminismo o la migración. Estas máscaras se cruzan con el uso del enmascaramiento por parte de los movimientos sociales como una herramienta opaca de transformación colectiva que rechaza las formas dominantes de representación política. Blas otorga a su trabajo una dimensión comunitaria y menciona específicamente a colectivos que trabajan con el ocultamiento del rostro como estrategia como pueden ser Occupy con el uso de la máscara de Guy Fawkes, los balaclavas rosas de las Pussy Riot o los pasamontañas Zapatistas.

La referencia de Blas a una *weaponization* (“armamentización”) del rostro es un reconocimiento de estos movimientos; lo que él llama el “poder del rostro colectivo” (Lee-Morrison, 2019, p. 151). Eliminando las características reconocibles del cara, l+s miembros de estos movimientos se convierten en una amenaza sin rostro para los sistemas asimétricos de poder a los que se enfrentan.

Las máscaras generadas por Blas son usadas posteriormente para intervenciones públicas y performances. Como, por ejemplo, la que tuvo lugar en junio de 2014 en la frontera de México. En este espacio se realizó una marcha, que bajo el nombre “Procesión de los dolores biométricos”, quería llamar la atención sobre la inmensa cantidad de datos biométricos que se recopilan en las fronteras y en particular en la frontera entre Estados Unidos y México.

***Fig. 3**. Zach Blas, Procession of Biometric Sorrows. 5 de junio de 2014, Ciudad de México, México, de Facial Weaponization Suite, 2014. Acción pública. Cortesía del artista.*

3.2. Maquillaje para camuflarse

Otra de las formas de esquivar los sistemas de reconocimiento facial es el maquillaje (Dantcheva, Chen y Ross, 2012) y algun+s artistas han elegido esta vía con altas posibilidades estéticas como espacio de exploración. Esta gama de acciones contempla desde pinturas de camuflaje ampliamente extendidas en usos militares, hasta toda una serie de fantasías festivas e imaginativas.

Adam Harvey es un artista e investigador especializado en vigilancia, privacidad y visión por ordenador. Ha creado todo tipo de dispositivos para evitar la vigilancia como "Off Pocket", una funda de teléfono que bloquea las señales inalámbricas; "Camoflash", un bolso antiparazzi equipado con un potente flash; o una colección de moda diseñada para evitar los drones o las cámaras térmicas. Pero uno de sus proyectos estrella es CV Dazzle, un camuflaje para el rostro diseñado para romper los sistemas de visión artificial sin dejar de ser perceptible para l+s observadores humanos. Los primeros patrones se diseñaron entre 2010 y 2013 constituyéndose como la primera técnica de camuflaje documentada que ataca con éxito un algoritmo de visión por ordenador. Estos diseños localizaban un punto de error que, cuando fue vulnerado, se extendió en cascada por toda la industria de seguridad. Las observaciones clave para las tecnologías de reconocimiento facial son la gran dependencia de las áreas oscuras alrededor de los ojos, la simetría, la estabilidad del puente nasal y la oscuridad debajo de la nariz. Mediante el uso de maquillaje y peinado, las áreas oscuras y claras se pueden revertir para reducir la probabilidad de detección. Con estos diseños se consiguió que una tecnología clave en el aparato de seguridad posterior al 11 de septiembre, anteriormente infalible, se viera frustrada por algo tan sencillo como el maquillaje y los peinados, de bajo costo o gratuitos, y accesibles a una amplia audiencia. Más tarde el algoritmo al que confundían[5] quedó obsoleto y Harvey diseñó unos nuevos looks para romper el reconocimiento facial de la red neuronal convolucional.

[5] La técnica se utilizó para romper el ampliamente utilizado (en ese momento) algoritmo de detección de rostros Viola-Jones mediante el uso de patrones en negrita para separar las características esperadas de los perfiles de detección de rostros (haarcascades). (https://adam.harvey.studio/cvdazzle/)

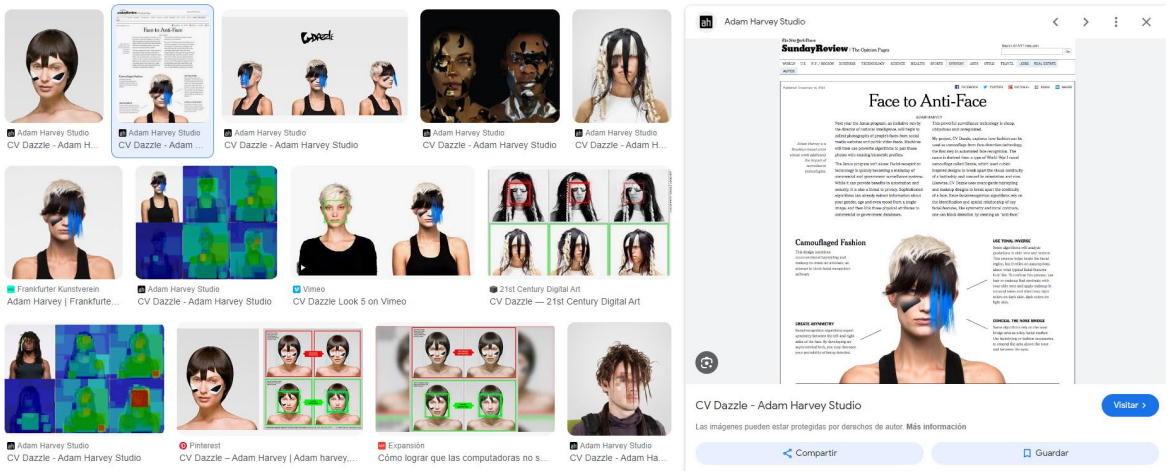

***Fig. 4**. Imágenes del proyecto CV Dazzle del artista Adam Harvey. Resultados de la búsqueda en google. 2024.*

El proyecto de Harvey, sin embargo, ha recibido críticas, como las que expresa Torin Monahan en un artículo sobre la estetización de la resistencia (2015). Este autor acusa al artista de promocionarse a sí mismo y generar una marca estética que centra la crítica en adornar el cuerpo con pinturas tribales pero que no tiene en cuenta el mayor escrutinio de poblaciones minoritarias y el sesgo racial de las tecnologías de vigilancia.

A partir de este proyecto de Adam Harvey nace el colectivo Dazzle Club (2019-2021) formado por cuatro artistas residentes en Londres que también han explorado las posibilidades del maquillaje como elemento de defensa contra la vigilancia y el uso de la tecnología de reconocimiento facial en el espacio público. Organizan caminatas por la ciudad en las que l+s participantes avanzan en silencio por las calles con maquillaje CV Dazzle. Aunque l+s participantes toman su tiempo en los diseños y verifican con aplicaciones que no se puedan someter a las tecnologías de reconocimiento facial, su objetivo principal no es tanto esquivar las cámaras de vigilancia sino crear una plataforma de discusión sobre estos temas (Lothian-McLean, 2020). En estas acciones urbanas reflexionan sobre los diferentes tipos de espacios públicos mientras se encuentran con público diverso, desde gente de negocios hasta estudiantes de arte, han sufrido detenciones e interrogatorios por personal de seguridad, e interactuado con compradores de centros compradores de centros comerciales o personas sin hogar en los callejones (Park, 2021).

***Fig 5**. Evie Price con el maquillaje de CV Dazzle aplicado. Fotografía tomada del Instagram de Dazzle Club. 3 de Marzo de 2020.*

En Rusia, el movimiento “Sledui”, también muestra rostros maquillados contra el reconocimiento facial en el espacio público, aunque su campaña tuvo menos recorrido porque fueron arrestad+s por la policía (Mas, 2020).

***Fig 6**. La artista Ekaterina Nenasheva siendo arrestada por la policía rusa por llevar maquillaje facial en el espacio público. Foto de Ivan Krasnov (Ivan KrasNov). Publicada en el facebook de la artista el 10 de febrero de 2020.*

3.3. Prestar un rostro

Dado que las intervenciones propuestas (máscaras, maquillajes, capuchas…) hacían parecer sospechos+s a l+s que las llevaban y podían ser motivo de represiones, al artista estadounidense Leo Selvaggio se le ocurrió la máscara prostética URME en 2014. Esta es una máscara 3D que replica el propio rostro del artista y que engaña a los sistemas de reconocimiento facial que identifican el rostro de la máscara, y no el de la persona que se esconde detrás de ella. El objetivo del proyecto es permitir a la gente presentar un rostro diferente al propio en público y ante las cámaras.

Leo explica que eligió su propio rostro porque no es ético poner a otra persona en riesgo y porque él es un hombre blanco privilegiado, y no hay nada que pase más desapercibido que un hombre blanco en un traje (Gallucci, 2015, p. 69).

La máscara se vende a precio de producción en la web del artista (http://www.urmesurveillance.com) con una declaración expresa de que no se obtienen beneficios por la venta del producto ya que el proyecto nace de la creencia de que tod+s deberían poder permitirse la protección contra la vigilancia.

***Fig 7**. Captura de pantalla del vídeo URME Surveillance: Indigogo campaign de Leo Selvaggio. https://www.urmesurveillance.com/*

4. CONCLUSIONES. EL DERECHO A SER ANÓNIM+

Como reseñan Pedro Cruz y Lidia García en su artículo "Cuerpo, máscara y biopolítica" el auténtico problema de la vigilancia no es que la razón gubernamental amplíe sus medidas de intervención sobre los cuerpos, sino que poc+s individu+s hay hoy que no quieran ser controlad+s (2019, p. 28). Quizás sea porque nos acogemos a la seguridad y comodidad que nos ofrece este control sin ser completamente conscientes de la contrapartida. Por este motivo, en la época de la vigilancia es interesante analizar para quién funciona la visibilidad y de qué forma lo hace. Hito Steyerl en su vídeo "How Not to be Seen: A Fucking Didactic Educational .MOV File" (2013) analiza irónicamente el contraste entre las capacidades sin precedentes de la tecnología para vigilar a los humanos e invadir la experiencia física, y la invisibilidad social y política de determinados sectores poblacionales. En este trabajo Steyerl va enumerando estrategias para volverse invisible, desde las más evidentes a las más disparatadas, incluyendo ser mujer y tener más de cincuenta años, o ser una persona desaparecida por ser enemiga de un estado.

Como hemos visto, las tecnologías de la vigilancia operan a través de una serie de políticas de visibilidad que están repletas de sesgos de raza, género y clase. Esto hace que determinadas personas sean escaneadas o sobrerrepresentadas por una arquitectura dominante de vigilancia. Existe una clara asimetría de poder sobre quiénes son los propietarios de la tecnología quienes los que producimos los datos. La sociedad de control no nos afecta a tod+s de la misma manera.

El ocultamiento del rostro, las estrategias de ofuscación para confundir y esquivar a los sistemas constituyen defensas legítimas para intentar evidenciar y, en la medida de lo posible, paliar estas asimetrías. El arte contribuye a estas estrategias desde una reflexión en muchas ocasiones irónica, en otras más comunitaria y pragmática, proponiendo un imaginario de la invisibilidad y el anonimato que se constituye como una alternativa a la sobreexposición.

Algun+s artistas eligen abordar la cuestión desde posicionamientos más tecnológicos desarrollando softwares o dispositivos capaces de contrarrestar o bloquear los algoritmos, otr+s desde una visión más política, social o comunitaria. El arte proporciona un amplio repertorio de prácticas que permiten esquivar y engañar a las tecnologías de control visual, pero sobre todo cuestionar de manera artística la normalización de la hipervigilancia.

Empleando una reflexión de Trevor Paglen, más que pensar la privacidad como un derecho individual, debemos entender el anonimato como un recurso público (Sojit Pejcha, 2020).

FUENTES REFERENCIALES

A. Cruz, P. y García, L. (2019). Cuerpo, máscara y biopolítica. Estrategias de opacidad en la era del big data. *ASRI. Arte y sociedad. Revista de investigación*, (17), 25-37.

Barret, D. (10 de julio de 2013). One surveillance camera for every 11 people in Britain, says CCTV survey. *The telegraph*. https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html

Bikolabs. (2021). Carta al Gobierno sobre la IA de reconocimiento facial. https://bikolabs.biko2.com/collections/carta

Brunton, F y Niessenbaum, H. (2015). *Obfuscation a user´s guide for privacy and protest.* The MIT Press.

Community Justice Exchange. (2022). From Data Criminalization to Prison Abolition. abolishdatacrim.org.

Crispin, S. (2014). Data-Masks Biometric Surveillance Masks Evolving in the Gaze of the Technological [Thesis, University of California] p. iv. http://www.sterlingcrispin.com/Sterling_Crispin_Data-masks_MS_Thesis.pdf

Dantcheva, A., Chen, C. y Ross, A. (2012). Can facial cosmetics affect the matching accuracy of face recognition systems?. *IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)* https://doi.org/10.1109/BTAS.2012.6374605

Deleuze, G. (1999). Post-scriptum sobre las sociedades de control. En *Conversaciones, 1972-1990*. (pp. 277-281). Pre-textos.

Dolgin, E. (9 de enero de 2019). AI face-scanning app spots signs of rare genetic disorders. *Nature*. https://www.nature.com/articles/d41586-019-00027-x

Gallucci, M. (2015). Interview to Leonardo Selvaggio. *Makeshift*, (12), 68-70.

Grother, P., Ngan, M. y Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. *National Institute of Standars and Technology, U.S. Department of Commerce.* https://doi.org/10.6028/NIST.IR.8280

Haraway, D. J. (1995). *Ciencia, cyborgs y mujeres. La reinvención de la naturaleza*. Cátedra.

Jain, A. K., Nandakumar, K. y Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters,* (79), 80-105. https://doi.org/10.1016/j.patrec.2015.12.013

Lee-Morrison, L. (2019). Portraits of Automated Facial Recognition *en Machinic Ways of Seeing the Face*. Bielefeldg. https://doi.org/10.1515/9783839448465

Lothian-McLean, M. (5 de febrero de 2020). These Activists Use Makeup To Defy Mass Surveillance. *I-d.vice.com.* https://i-d.vice.com/en_uk/article/jge5jg/dazzle-club-surveillance-activists-makeup-marches-london-interview

Mas, L. (14 de febrero de 2020). Russian artists wear anti-facial recognition make-up… and get arrested. *The observers*. https://observers.france24.com/en/20200214-russian-artists-facial-recognition-makeup-arrested

Monahan, T. (2015). The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance. *Communication and Critical/Cultural Studies, 12*(2), 159-178. https://doi.org/10.1080/14791420.2015.1006646

Mozur, P. (14 de abril de 2019). One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. *The New York Times.* https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Murgia, M. (6 de junio de 2019). Microsoft quietly deletes largest public face recognition data set. *Financial Times.* https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2

Park, B. (2021). Countervisuality for a Gentrifying City Center: Structuring Systems of Surveillance Through Architecture. Conferencia impartida en ECA (Eastern Communication Association annual conference) https://ecacomm.org/aws/ECA/asset_manager/get_file/553896?ver=1

Reinhuber, E. (2024). Outsmarting the algorithm or leaving the grid through surveillance artivism. *Artnodes,* (33), 1-8. https://doi.org/10.7238/artnodes.v0i33.418372

Roberts, C. (2007). Biometric attack vectors and defences. *Computers & Security, 26*(1), 14-25. https://doi.org/10.1016/j.cose.2006.12.008

Rollet, C. (13 de junio de 2018). In China's Far West, Companies Cash in on Surveillance Program That Targets Muslims. *Forein Policy.* https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companies-cash-in-on-surveillance-program-that-targets-muslims/

Sojit Pejcha, C. (15 de septiembre de 2020). Trevor Paglen wants you to stop seeing like a human. *Document.* https://www.documentjournal.com/2020/09/trevor-paglen-wants-you-to-stop-seeing-like-a-human/

Steyerl, H. (2013). How Not to be Seen: A Fucking Didactic Educational. MOV File [Archivo de vídeo]]https://www.moma.org/collection/works/181784