Sousveillance art: artivismo como estrategia de enfrentamiento a la vigilancia en línea*

Lorena Ferreira Alves**
Antenor Ferreira Corrêa***

[RESUMEN]

El propósito de este artículo fue presentar los conceptos de sousveillance y dataveillance, así como reflexionar sobre las formas de artivismos propuestas para interrogar y resistir a la sociedad de vigilancia. Observamos, en la sociedad contemporánea, una relación inversamente proporcional entre privacidad y tecnología. Esto ocurre por la conveniencia que conllevan los complejos sistemas de vigilancia en línea para los cuales regalar datos personales se ha convertido en la moneda para vivir en un mundo conectado. En medio de esta situación, consideramos algunas obras en el campo del sousveillance art con el fin de comprender cómo los artistas se han posicionado en esta situación. Las consideraciones que se proponen se basan en el análisis de obras de arte basadas en algunos textos que abordan los conceptos de privacidad y vigilancia.

Palabras clave: sousveillance art, artivismo, estética de la vigilancia, privacidad.

Doi 10.11144/javeriana.mavae18-2.savl
Fecha de recepción: 29 de octubre de 2022
Fecha de aceptación: 4 de marzo de 2023

* Artículo de investigación.

** Doctora en Artes por la Universidade de Brasília y en Historia y Artes por la Universidad de Granada, magíster en Música por la Universidade Federal de Goiás y licenciada en Música por la misma universidad. Actualmente trabaja con arte sonoro y arte y vigilancia. Este artículo forma parte de los resultados de su tesis doctoral realizada en convenio de cotutela entre la Universidade de Brasília y la Universidad de Granada, financiada por la beca de estudios doctorales de la CAPES, Brasil.
ORCID: https://orcid.org/0000-0002-2890-201X
Correo electrónico: lorenatrack@gmail.com

*** Compositor, percusionista, investigador y profesor asociado de la Universidade de Brasília. Tiene un posdoctorado de la Universidad de Granada (beca Fundación Carolina y Grupo Tordesillas), posdoctorado en la Universidad de California, Riverside (beca CAPES), doctorado en Música por la Escola de Comunicações e Artes da Universidade de São Paulo (ECA-USP) (beca CAPES). Desde 2018 coordina el Laboratório de Pesquisa em Arte Computacional (MediaLab/UnB). Recibe beca (nivel PQ2) del Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).
ORCID: https://orcid.org/0000-0003-0257-3059
Correo electrónico: antenorfc@unb.br

CÓMO CITAR: Ferreira Alves, Lorena y Antenor Ferreira Corrêa.2023.Sousveillance art: Artivismo como estrategia de enfrentamiento a la vigilancia en línea". *Cuadernos de Música, Artes Visuales y Artes Escénicas* 18 (2): 164-179. https://doi 10.11144/javeriana.mavae18-2.savl

Sousveillance Art: Artivism as a Strategy to Confront Online Surveillance

Sousveillance art: artivismo como estrategia para enfrentar à vigilância online

[ABSTRACT]

This article aims to introduce the concepts of sousveillance and dataveillance, as well as reflect on the proposed forms of artivism to question and resist the surveillance society. In contemporary society, there is an inversely proportional relationship between privacy and technology. This is because complex online surveillance systems offer convenience and giving away personal data has become the currency for living in a connected world. In the midst of this situation, the article examines some works in the field of sousveillance art to understand how artists have positioned themselves in this context. The considerations proposed are based on the analysis of artworks and texts that address the concepts of privacy and surveillance.

Keywords: sousveillance art, artivism, aesthetics of surveillance, privacy.

[RESUMO]

O objetivo deste artigo foi apresentar os conceitos de sousveillance e dataveillance, bem como refletir sobre as formas de artivismo propostas para interrogar e resistir à sociedade de vigilância. Observamos, na sociedade contemporânea, um relacionamento inversamente proporcional entre privacidade e tecnologia. Isso acontece pela conveniência dos complexos sistemas de vigilância online para os quais o fornecimento de dados pessoais se tornou moeda corrente para viver em um mundo conectado. Em meio a essa situação, consideramos algumas obras no campo do sousveillance art a fim de compreender como os artistas têm-se posicionado nessa situação. As considerações propostas partem da análise de obras de arte baseadas em alguns textos que abordam os conceitos de privacidade e vigilância.

Palavras-chave: sousveillance art, artivismo, estética da vigilância, privacidade

▪ CUAD. MÚSIC. ARTES VIS. ARTES ESCÉN. ▪ VOL. 18 - 2 ▪ PP. 218 ▪ JULIO - DICIEMBRE 2023 ▪ BOGOTÁ, D.C., (COLOMBIA) ▪ ISSN 1794-6670 ▪

Introducción[1]

> Una palabra que todos usan, pero que es realmente difícil de definir, es *privacidad*. Las cosas se complican aún más cuando pensamos en la existencia misma de la privacidad en el ámbito de internet. ¿Existe tal cosa como la privacidad en línea?

Una situación habitual en la vida diaria de los usuarios de internet es tener que hacer clic en los cuadros de texto para autorizar el uso de *cookies* por parte del sitio web al que se accede. Ocurre que, por prisas, ganas o incluso por la necesidad de acceder a cualquier página o sitio web, acabamos autorizando el uso de estas *cookies*, muchas veces sin pensar en las consecuencias que este permiso puede traer. Lo que algunos no saben, sin embargo, es que estas *cookies* pueden suponer riesgos para la privacidad del usuario.

Pero, para lidiar con las complejidades de la (falta de) privacidad en internet, es necesario definir de qué estamos hablando cuando hablamos de privacidad. Una definición completa de privacidad todavía no existe. Las áreas de biología, derecho y sociología, por ejemplo, trabajan con diferentes definiciones del sustantivo "privacidad" y del adjetivo "privado". En el capítulo titulado "What is Privacy?", Alexandra Rengel (2013) cita a varios autores que intentaron una definición objetiva de privacidad, pero el problema está lejos de resolverse. Citando a Robert Post, profesor de derecho en la Facultad de Derecho de Yale, Rengel señala que "la privacidad es un valor tan complejo, tan enredado en dimensiones competitivas y contradictorias, tan lleno de significados diversos y distintos, que a veces me desespero si esta se puede abordar de manera útil" (31).

Jan Holvast, a su vez, realizó uno de los informes históricos más completos sobre privacidad, habiendo identificado los diversos aspectos a través de los cuales se ha planteado el tema. En su análisis, las discusiones sobre privacidad involucran puntos de partida y bases diversas, como la necesidad de privacidad, el derecho a la privacidad, la invasión de la privacidad, las funciones de la privacidad o, incluso, la protección legal de la privacidad.

Sin embargo, varios autores coinciden en que la publicación de "The Right to Privacy", de Samuel Dennis Warren y Louis Demitz Brandeis en 1890, en *Harvard Law Review*, se convirtió en un hito en la historia del derecho en los Estados Unidos y, en consecuencia, influyó en otros países (Barreto y Pereira dos Santos 2006; McDougall y Hansson 2002; Vieira 2016). Este texto fundó los principios constitucionales estadounidenses y generó la definición de privacidad adoptada hasta hoy: "the right to be let alone", que literalmente sería "el derecho a ser dejado solo". La forma adoptada en el poder judicial brasileño, por ejemplo, es "el

derecho a ser dejado en paz". Respecto de la definición de privacidad, en Perú, la Constitución solo se refiere a la "intimidad personal" y se entiende como una esfera personal a la que el Estado o una tercera persona no puede ingresar sin el previo consentimiento. En la actualidad, principalmente por los aspectos relacionados con las prácticas en internet, el concepto de *privacidad* tuvo que ampliarse y pasó a referirse al "estado o condición relacionada con las conductas y relaciones íntimas en las que el sujeto controla el acceso y toma decisiones autónomas" (McDougall y Hansson 2002, 5).

La privacidad, tratada legalmente como un derecho ciudadano, termina generando una serie de interrogantes. ¿Dónde termina la esfera privada y comienza el derecho a la información pública? ¿Cuáles son los límites de la privacidad de una personalidad pública? ¿Tienen los funcionarios del Gobierno derecho a la privacidad cuando ejercen funciones encomendadas públicamente? ¿Tiene derecho al olvido un sujeto que sea agente de un acto público atroz? ¿Tiene el Estado derecho a utilizar todos los medios para obtener información privada de los ciudadanos?

Sin embargo, el derecho a la privacidad se ha transformado radicalmente después de algunos ataques terroristas que han tenido lugar en varios países. Uno de los momentos que más impactó la garantía de este derecho y llevó al mundo a una nueva condición jurídica fue el atentado contra las Torres Gemelas del complejo World Trade Center en Nueva York (Estados Unidos), el 11 de septiembre de 2001. Este atentado, supuestamente llevado a cabo por el grupo extremista islámico Al Qaeda, ha provocado que los ciudadanos reconsideren su derecho a la privacidad a cambio de la seguridad que podría brindar la vigilancia ubicua e invasiva. Según Rengel (2013), "la aprobación de la legislación antiterrorista que afecta las libertades civiles después del 11 de septiembre no se limitó a los Estados Unidos (174). Unas semanas después de los ataques del 11 de septiembre, el entonces presidente George Bush firmó lo que se conoció como la Ley Patriota (Patriot Act), un documento con más de 300 páginas en las que se promulgó una legislación cuyo objetivo principal era "mejorar las habilidades de aplicación de la ley de los Estados Unidos para detectar y detener el terrorismo. El nombre oficial de la Ley Patriótica es Unión y fortalecimiento de la América, que proporciona herramientas adecuadas para interceptar y obstruir el terrorismo" (Patriot Act 2017). La cuestión principal es que la promulgación de este y de otros documentos relacionados llevó al mundo a una nueva condición de miedo y restricción de libertades y derechos, es decir, la llamada sociedad de la vigilancia, donde el derecho a la privacidad fue profundamente cambiado.

Obviamente, muchos pensadores, activistas de derechos humanos y artistas cuestionan y disputan los supuestos beneficios que trae consigo la limitación de las libertades y los derechos de los ciudadanos impuestos por las leyes destinadas a combatir el terrorismo. Entre ellos, una de las exposiciones que cuestionó el derecho de Gobiernos y corporaciones a recolectar y almacenar información de vigilancia en los distintos medios fue *Watching You, Watching Me: A Photographic Response to Surveillance*.[2] El texto de la presentación de esta exposición lo dejó claro:

> A medida que los Gobiernos y las empresas de todo el mundo amplían sus esfuerzos para rastrear las comunicaciones y actividades de millones de personas, esto no solo amenaza nuestro derecho a la privacidad, sino que también abre la puerta para que la información se recopile y utilice de manera represiva, discriminatoria, y congelen la libertad de discusión y expresión. (Museum für Fotografie 2017)

Entre las diversas obras expuestas, la serie *Blue Sky Day* del galardonado fotógrafo belga Tomas van Houtryve invita a pensar en los mecanismos y las tecnologías de vigilancia actuales con los que convivimos sin ni siquiera darnos cuenta. Dicha serie es un conjunto de fotografías aéreas tomadas por un dron (vehículo aéreo no tripulado y controlado a distancia). Houtryve

usó el dron para grabar imágenes de lugares en los Estados Unidos similares a los que fueron el objetivo del ataque en el extranjero. Así, nos obliga a reflexionar no solo sobre la vigilancia o la guerra, sino también sobre los efectos que provocan estas acciones a través de la narrativa de las fotografías, ya que esta incita a pensar que los objetivos bombardeados en el exterior por drones estadounidenses también existen en los Estados Unidos y están bajo vigilancia, sujetos al mismo tipo de acción militar. La figura 1 muestra una de las imágenes de la serie *Blue Sky Day* titulada *Authorized overflight zone* (2013). La serie de Houtryve recibió varios premios, como el ICP Infinity de fotoperiodismo, y fue elegida entre las 10 fotografías más importantes de 2014 por la revista *Time*.

Teniendo como punto de partida este tipo de actitud artística que se denomina artivismo, pretendemos reflexionar sobre la sociedad de la vigilancia a través de la idea de *sousveillance art* (tema que se comenta a continuación) como una de las formas de minimizar los efectos generados por la vigilancia ubicua, ya que, como veremos más adelante, es prácticamente imposible evitarla. Por tanto, nos cuestionamos sobre cómo se han posicionado los artistas en esta situación. Será interesante, sin embargo, antes de entrar en el tema de la contravigilancia, definir y contextualizar algunos términos esenciales para sustentar la reflexión política y artística.

Sociedad de la vigilancia

La sociedad de la vigilancia, "una sociedad donde la tecnología de vigilancia es ampliamente utilizada para monitorear las actividades diarias de las personas" ("Surveillance society" 2023), se refiere así a una rama del monitoreo de las acciones humanas que cubre todos los ámbitos de la vida de un individuo, que van más allá del propósito inicialmente aplicado a estas tecnologías introducidas en la vida social cotidiana, es decir, la seguridad de los ciudadanos. Las tecnologías de vigilancia, como las cámaras de televisión de circuito cerrado, la captura y grabación de sonido y el monitoreo de la ubicación, se han convergido e incorporado en dispositivos de comunicación y servicios de asistencia personal, como el *smartphone*, iPhone o Siri. Actualmente, interactuamos con las interfaces de monitorización de estos dispositivos, los llevamos a nuestros hogares y los vestimos en nuestro cuerpo como instrumentos para experimentar los mundos personalizados que nos ofrecen.

¿Cómo llegamos a aceptar e incorporar estas tecnologías de vigilancia que pueden influir en nuestros comportamientos y elecciones? Es posible señalar hechos que se han convertido en gran parte responsables de la inserción de vigilancia de datos personales y la invasión de la privacidad de los usuarios de internet. Uno de los hechos principales, como se mencionó, fue la introducción de la vigilancia masiva de los medios a escala mundial después de los ataques del 11 de septiembre de 2001 en los Estados Unidos. Como consecuencia, el discurso a favor de la seguridad global elaborado por sectores del Gobierno estadounidense definió formas de aplicar tecnologías de vigilancia de datos en internet, inicialmente con el respaldo de ciudadanos estadounidenses que aceptaron el argumento de los líderes gubernamentales y renunciaron a la privacidad a cambio de la supuesta seguridad que las tecnologías de vigilancia ofrecen. Lacaze (2016), considerando la propaganda llevada a cabo por las autoridades estadounidenses durante la implementación de la vigilancia masiva de los medios de comunicación, cree que este objetivo se logró, en gran parte, debido al establecimiento de un ambiente de miedo y urgencia en la prevención y el combate a otros ataques terroristas y ciberataques. De esta forma, los Estados Unidos se han posicionado como la autoridad antiterrorista, promoviendo la vigilancia masiva, reforzada por la recopilación de datos en internet, como la única

Figura 1. Tomas van Houtryve, Authorized overflight zone, 2013, de la serie Blue Sky Days
Fuente: "Blue Sky Days" (2013).

forma efectiva de establecer la protección de los ciudadanos. Como resultado, la regulación de la vigilancia amplia y general se implementó en la Ley Patriótica, que legitimó la práctica de interceptar teléfonos y correos electrónicos por parte de agencias y organismos de seguridad estadounidenses, como la National Security Agency (NSA) y el Federal Bureau of Investigation (FBI).

A partir de ello, el uso de los datos de navegación de los usuarios y su información personal, como nombre, edad, ubicación, entre otros, pronto se aplicó como un procedimiento para predecir posibles audiencias por parte de las empresas que serían capaces de trazar perfiles en función de las preferencias de los usuarios, y así apuntar contenido publicitario para ofrecer productos. Precisamente por esta razón, la mayoría de los servicios disponibles en internet, como los chats, las redes sociales y los sitios de búsqueda, operan de acuerdo con la gestión algorítmica de los datos interceptados, lo que convierte a internet en la tecnología de vigilancia más poderosa desde el punto de vista de la eficiencia de monitoreo de datos personales.

El consentimiento para la vigilancia de los datos personales, ya en la computadora personal, ya en los dispositivos portátiles de comunicación, viene dado por la conveniencia que estas tecnologías pueden ofrecer. Así, se vuelve cada vez más difícil optar por no formar parte de una sociedad de vigilancia o, incluso, intentar revertir la trayectoria del desarrollo tecnológico que tiende a una vigilancia cada vez más incisiva. Considerando, por ejemplo, que muchos servicios (como la compra de boletos) tienen acceso disponible a través de sitios web o aplicaciones en línea, las cuales, además de requerir datos de usuario, se pueden rastrear fácilmente. Ante este contexto, podemos prever que, con la implantación definitiva del internet de las cosas (IoT, por sus siglas en inglés) y su incorporación en las ciudades inteligentes, la opción de "no estar *online*" prácticamente no existirá. Jonas (2015) comenta sobre cómo la sociedad de vigilancia es irresistible:

Figura 2. Tracking Transience 3-channel video on 27 monitors as installed at Made in NY Media Center by IFP Brooklyn, New York 2014. http://elahi.wayne.edu/elahi_miny.php

> Una sociedad de vigilancia es inevitable e irreversible. Más interesante aún, creo que una sociedad de vigilancia también resultará irresistible. Este movimiento no está siendo impulsado únicamente por los Gobiernos, sino principalmente por los consumidores, usted y yo, ya que adoptamos con entusiasmo un número cada vez mayor de bienes y servicios irresistibles, a menudo sin saber qué información personal se recopila o cómo podría terminar siendo utilizada. (93)

Si bien la preocupación por la privacidad se expresa cuando se habla de vigilancia, se convierte en un desafío ubicar en una sociedad de vigilancia lo que se considera información pública o privada. Los datos sobre el comportamiento digital y la exposición de la intimidad por parte del propio usuario en internet son monitoreados por empresas y posteriormente compartidos con otras. De esta manera, se pueden observar dos niveles de acceso e intercambio de datos personales: a) los datos detallados de huellas digitales e información de registro que el usuario deja en la web y son recopilados por corporaciones, y b) la información personal generada por el propio usuario para indicar su presencia en redes sociales. Dentro de este entorno monitoreado, la privacidad es prácticamente inexistente debido a que no siempre somos conscientes de las formas en que nuestros datos se recopilan y comparten entre otros usuarios o grupos de socios comerciales.

Ante la casi imposibilidad de permanecer oculto, ¿cuáles serían las estrategias de resistencia de los ciudadanos preocupados, en general, por los derechos y las libertades civiles y, en particular, por el derecho a la intimidad? Algunos estudiosos sostienen que la propuesta de revertir la vigilancia, también llamada *sousveillance*,[3] es una de las estrategias para lidiar con la sociedad de la vigilancia. En otras palabras, hacer del observado un observador de sí mismo, y así generar una "visibilidad total" (véase más abajo el caso de Hasan Elahi).

La problematización de la vida en una sociedad de vigilancia no es nueva. Desde, al menos, 1949, año de la publicación de la ficción distópica de George Orwell, *1984* (que, además de reflexionar sobre las consecuencias de un Estado totalitario, autoritario y represivo que mediante una vigilancia omnipresente controlaba el comportamiento de las personas y la sociedad, acuñó la expresión *big brother*), algunos artistas han planteado preguntas y ofrecido formas de resistencia al control total de los Gobiernos. Sin embargo, con la creciente omnipresencia de los dispositivos de vigilancia, visibles e invisibles, una nueva forma de tratar y responder a esta situación se ha denominado estética de la vigilancia (Bruno et al. 2012) o arte de la vigilancia.

Sousveillance: arte de la contravigilancia

¿Qué pasaría si en lugar de intentar dificultar o impedir que los organismos gubernamentales y las instituciones comerciales accedan a nuestra información personal simplemente informáramos de antemano a estos organismos de nuestros movimientos, destinos y actividades realizadas en cada instante? En otras palabras, ¿si en lugar de existir como observados en secreto nos convirtiéramos en proveedores de datos sobre nosotros mismos? Esta es exactamente la base de la propuesta artística del proyecto *Tracking Transience: The Orwell Project*, del artista Hasan Elahi.

En lugar de exigir la preservación de su derecho a la privacidad, Elahi decidió el camino contrario, es decir, paradójicamente, renunciar a su privacidad para sentirse más seguro. De este modo, creó un sitio web en el que, de forma voluntaria y constante, facilitaba información sobre

Figura 3. Heather Dewey-Hagborg, Stranger Visions. Installation at Laznia Museum of Contemporary Art in Gdansk, Poland, 2016. https://deweyhagborg.com/projects/stranger-visions

todas sus actividades diarias. Elahi, nacido en Bangladés y nacionalizado estadounidense, es actualmente profesor del Departamento de Arte de la Universidad de Maryland (Estados Unidos). Sin embargo, seguía siendo un desconocido cuando, en 2002, fue detenido en el aeropuerto de Detroit por una acusación errónea de almacenamiento de explosivos. Desde ese momento, fue detenido e interrogado por Immigration and Naturalization Service (INS) durante seis meses. Los interrogatorios se centraron en cuestionar su paradero en los días anteriores y posteriores a los atentados del 11 de septiembre. Si bien las acusaciones fueron finalmente retiradas, con este incidente, Elahi fue fichado por el FBI, lo que hizo su vida mucho más difícil (era detenido con frecuencia por los guardias de seguridad en aeropuertos y estaciones de tren) e insegura (por los prejuicios generados contra los grupos étnicos tras los atentados terroristas). Fue entonces cuando Elahi decidió renunciar a su privacidad y proporcionar preventivamente no solo al FBI, sino a todos los usuarios de internet, informaciones sobre su paradero y actividades.

La figura 2 muestra una de las obras de este proyecto, una instalación con 27 monitores de varias videograbaciones de las actividades de Elahi expuestas en *Made in NY Media Center, New York* (2014). Esta y otras obras resultantes del proyecto fueron expuestas en diversos festivales y exposiciones de arte de todo el mundo. Elahi ha recibido premios y honores, así como una beca de la Fundación Guggenheim. Además, su presentación en TED Talks "FBI, here I am" es citada a menudo por el impacto y la relevancia de su manifiesto artístico que desafía la vigilancia en la sociedad actual.

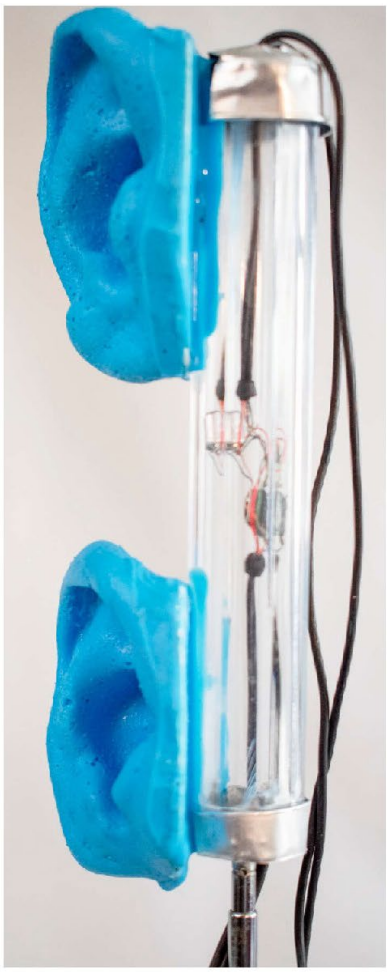
Varias propuestas, como la de Elahi, para pensar, cuestionar y combatir la sociedad de la vigilancia impuesta a los ciudadanos del mundo han surgido en diversos segmentos artísticos. Históricamente, el cuestionamiento artístico sobre la privacidad y la vigilancia resultante del uso de la tecnología puede remontarse, al menos, a los inicios del videoarte, a finales de la década de 1960. Obras como *Sleep* (1964) y *Outer and Inner Space* (1966) de Andy Warhol, *Claim* (1971) y *Seedbed* (1972) de Vito Acconci, entre otras, fueron consideradas obras transgresoras porque presentaban al público aspectos y cuestiones sobre la privacidad. Muchos de estos artistas han hecho un uso explícito de las grabaciones de video adquiridas en los llamados *closed-circuit television* (CCTV), como Jill Magid (*Evidence Locker*, 2004).

Figura 4. David Rokeby, dos capturas de pantalla de Sorting Daemon, 2003. http://www.davidrokeby.com/sorting.html

Más recientemente, con el desarrollo de las tecnologías de vigilancia, la invasión de la privacidad es mucho más contundente y ubicua de lo que, incluso, los analistas más pesimistas podrían sospechar. El creciente contexto de vigilancia en el que estamos inmersos ha llevado a la creación de obras artísticas que precisamente pretenden debatir sobre las tecnologías, los mecanismos, las ideologías y las imposibilidades de la privacidad. Esta motivación ha formado y forma parte del manifiesto estético de varios artistas y ha llegado a constituir un tipo de creación denominado *surveillance art*, cuyo rasgo distintivo es el uso explícito de las propias tecnologías diseñadas para vigilar y registrar la conducta cotidiana de los ciudadanos, sea esa conducta vigilada en las calles o en entornos digitales virtuales. El objetivo principal del *surveillance art* (también llamado *artveillance*) es reflejar y problematizar el proceso de vigilancia en sí mismo, así como las tecnologías creadas para lograrlo. Varios artistas se hacen eco de este manifiesto, como los mencionados Hasan Elahi y Tomas van Houtryve, junto con los que podríamos mencionar a Trevor Paglen, Benjamin Males, Christian Moeller y Robert Spence (alias *eyeborg*), por ejemplo. Del mismo modo, Bruno et al. (2012) ofrecen un importante panorama de algunas obras de artistas latinoamericanos, así como exposiciones significativas en el campo de la estética de la vigilancia.

Una de las artistas más contundentes en el cuestionamiento de las tecnologías de vigilancia es Heather Dewey-Hagborg, sobre todo con su trabajo en la intersección del arte y la ciencia. Uno de sus proyectos más incisivos es *Stranger Visions*, en el que fue a lugares públicos de Nueva York, como baños, salas de espera, estaciones y coches de metro, para recoger cabellos, restos de uñas, chicles y colillas desechados por las personas. Utilizó estas muestras para extraer el ADN y, a partir del código genético resultante, generar una especie de máscara impresa en una impresora 3D creada con las características probables de la persona que desechó el material (figura 3). Según Dewey-Hagborg, "el proyecto pretendía llamar la atención sobre el desarrollo de la tecnología forense basada en el fenotipado del ADN, el potencial de una cultura de vigilancia biológica y el impulso del determinismo genético" ("Stranger Visions" 2009-2023).

De igual manera, el artista canadiense David Rokeby instiga a cuestionar el uso de los aparatos de vigilancia para clasificar a las personas en grupos predeterminados. La instalación *Sorting*



v
v

Figura 5. Lorena Ferreira, Personal Auricularveillance, 2020. https://www.premiopipa.com/lorena-ferreira/

Daemon de 2003 (figura 4), comisionada e instalada en el Instituto Goethe de Toronto, consiste en una cámara instalada dentro de la Galería Goethe, pero apuntando hacia la calle, desde donde capta imágenes de los transeúntes. A través de un ordenador conectado a la cámara, identifica y aísla del fondo la imagen de las personas que pasan. Luego, esta persona es separada y agrupada siguiendo un criterio de color y tamaño. Las diversas imágenes extraídas, separadas y agrupadas se proyectaron en una pared del interior de la galería. Rokeby aclara que "*Sorting Daemon* es una instalación *site-specific* que surgió de mi preocupación por el creciente uso de sistemas automatizados para elaborar perfiles de personas como parte de la 'guerra contra el terrorismo' y es un intento de ayudar a plantear preguntas sobre los usos adecuados de la tecnología" ("Interactive Installations: Sorting Daemon (2003)" 2013).

Hay que observar también varios trabajos en el campo del arte y vigilancia elaborados como forma de discutir la ausencia de privacidad en el entorno del ciberespacio. Por ejemplo, la obra *Personal Auricularveillance*, de la artista brasileña Lorena Ferreira, puede tomarse como otra forma de trabajo artístico que aborda la vigilancia de datos en internet y la invasión de la privacidad. El objeto *Personal Auricularveillance* fue desarrollado para ser un producto que ofrece a los usuarios monitoreados opciones para engañar, prevenir o mejorar la vigilancia sonora practicada por las grandes empresas que manejan *big data*. Este producto surge como una alternativa para brindar relaciones entre el sujeto observado y el sistema que lo vigila, deconstruyendo la posición de impotencia y vulnerabilidad que los usuarios encuentran ante la vigilancia incisiva e ininterrumpida que se da en las tecnologías mediáticas actuales.

El trabajo analiza la especulación actual sobre la vigilancia sonora de los dispositivos de teléfonos inteligentes que "escuchan nuestras conversaciones" para capturar los deseos de los consumidores y orientar los anuncios. Los rumores de que Facebook nos escucha a través del micrófono de tu teléfono han persistido durante los últimos años. De manera similar, en abril de 2019, los rumores de una posible vigilancia de sonido operada por la tecnología de asistente virtual Alexa, desarrollada por Amazon, fueron expuestos por la empresa de tecnología y análisis de datos Bloomberg, que afirmó que los empleados de Amazon tendrían acceso a las grabaciones de voz de los usuarios de esta herramienta transcribiendo en texto. Como propuesta para boicotear y confundir la forma en que los guardias de seguridad interpretan nuestros comportamientos en línea para crear perfiles de consumo, la obra *Personal Auricularveillance* ofrece la posibilidad de que el usuario seleccione, bloquee o amplifique la captura de los sonidos monitoreados.

La instalación tiene prótesis de oído humano adheridas a los micrófonos de los teléfonos celulares (figura 5). El artista ha desarrollado tres variaciones de este "producto": el *Personal Auricularveillance One*, que permite mejorar la calidad del sonido de vigilancia procesado por el *smartphone* o iPhone; el *Personal Auricularveillance Privacy*, que bloquea la entrada de sonidos ambientales y así garantiza la privacidad sonora, y el *Personal Auricularveillance Ultra*, que, además de ofrecer las capacidades del *Personal Auricularveillance One* y el *Personal Auricularveillance Privacy*, también permite cambiar los sonidos que se están monitoreando.

Consideraciones finales

La historia de la privacidad deja clara la relación inversa entre privacidad y tecnología. Cuanto más evoluciona la tecnología, más sofisticados son los medios de vigilancia y menos privacidad se tiene. Desde el uso de las escuchas telefónicas, ya detectadas en 1918,[4] pasando por los circuitos cerrados de cámaras hasta las complejas técnicas de vigilancia de datos, el derecho a la intimidad se ha ido desvaneciendo. La política aplicada tras los atentados terroristas, como

los de Nueva York (2001), Madrid (2004) y Londres (2005), demuestra que el derecho a la intimidad depende de la determinación del Gobierno. Sin embargo, como subraya Holvast (2007), "el deseo político global está más orientado hacia el uso eficaz y eficiente de la tecnología en la lucha contra la delincuencia y el terrorismo que hacia la protección de la privacidad" (738). Los avances tecnológicos en la tecnología de la información habían engendrado un nuevo contexto denominado sociedad de la información (*information society*), que se consideraba el resultado del progreso tras el modelo social industrial, que a su vez sucedió al modelo agrícola. Sin embargo, la aceptación de estas tecnologías, sea cual sea la justificación de este consentimiento, tuvo como consecuencia la aparición de un nuevo modelo social denominado sociedad de la vigilancia (*surveillance society*). En las fatídicas palabras de este autor, "la ubicuidad de la tecnología y la aceptación de políticas y leyes para recopilar, almacenar y utilizar prácticamente todos los datos personales está convirtiendo la sociedad de la información en una sociedad de la vigilancia" (766).

Una sociedad de la vigilancia produce un comportamiento social basado en las formas en que los individuos y las comunidades hacen frente a la vigilancia. Estas formas son impuestas por los Gobiernos y también creadas por los ciudadanos. La sociedad de la información, a su vez, se entiende como un modelo de comportamiento, conducta y actitudes basado económica, cultural y políticamente en la manipulación e integración de la información. Los motores de esta estructura social son las tecnologías de la información y la comunicación (TIC) que multiplican rápidamente la información y provocan transformaciones en todos los aspectos de la organización social, como la educación, la economía, la salud, la beligerancia, la ideología, entre otros (Beniger 1986).

El modelo de la sociedad de la vigilancia acaba engendrando ciertos binarismos, por ejemplo, la vigilancia perceptible e imperceptible. Este antagonismo entre lo que vemos y lo que se nos oculta apunta a dos modalidades de vigilancia: la visible (cámaras de circuito cerrado, monitores, detectores de metales, etc.) y la invisible (cintas telefónicas, dispositivos de medición de audiencia instalados en los televisores, espionaje por satélite, drones, *dataveillance*, etc.). La pregunta que hay que hacerse, y que en mayor o menor medida han planteado ampliamente los artistas que trabajan en la *artveillance*, es ¿cómo responden las personas de diferentes culturas y contextos sociales a la vigilancia constante? Y una de las principales preocupaciones "es que la gente se vuelve más conformista al suprimir su individualidad" (Holvast 2007, 742). Y esta supresión de la individualidad diluida en un colectivo engendrado a partir de los datos recogidos se efectúa, de hecho, por la abdicación del derecho a la privacidad.

Tras la movilización global desarrollada por los Estados Unidos a favor del uso de las tecnologías de vigilancia por parte de sus agencias de seguridad, se sacrificó la pérdida de privacidad a favor de un supuesto bien mayor: la seguridad global. Pronto, con la implantación de la vigilancia masiva y ubicua, las tecnologías de vigilancia de datos empezaron a utilizarse con otros fines, como la promesa de mejorar los resultados de las búsquedas de contenidos en internet. Por ejemplo, empresas como Google, que desarrollan productos para la navegación web, han mejorado las tecnologías de monitoreo en la red mundial como una forma de administrar los datos personales, la ubicación y las huellas de navegación a los usuarios del perfil para distribuir los resultados de búsqueda de manera personalizada. Desde diciembre de 2009, según Pariser (2012), la realización de búsquedas en Google también ha comenzado a producir resultados personalizados para cada usuario, mediante algoritmos que calculan los productos que más se acercan a sus preferencias y posibles necesidades. Esto significa que la misma búsqueda realizada por dos usuarios con perfiles diferentes puede revelar resultados diferentes.

No se puede perder de vista que vivimos en una sociedad, y la vida social implica restricciones, incluso en relación con los límites de la privacidad. En este sentido, Holvast (2007) comenta que "vivir en comunidad significa, por definición, estar involucrado con los demás" (741). Así, sigue siendo válida, o debería serlo, la antigua concepción del estado de derechos y deberes.

▪ CUAD. MÚSIC. ARTES VIS. ARTES ESCÉN. ▪ VOL. 18 - 2 ▪ PP. 218 ▪ JULIO - DICIEMBRE 2023 ▪ BOGOTÁ, D.C., (COLOMBIA) ▪ ISSN 1794-6670 ▪

Figura 6. Bansky, grafiti sin título.
https://www.banksy.co.uk/

No obstante, lo que muestran varios estudios es precisamente el desvanecimiento del derecho a la privacidad en sus dos dimensiones: la privacidad territorial y corporal (*territorial and bodily privacy*) y la privacidad informacional, es decir, la relativa a la recolección, el almacenamiento y el tratamiento de datos personales.

Ante esta situación, los Gobiernos y las empresas han puesto en marcha un procedimiento que se ha dado en llamar contravigilancia. De este modo, las empresas invierten grandes sumas de dinero para tratar de evitar el espionaje digital y la vigilancia de datos (*dataveillance*) mediante medidas y tecnologías de seguridad, denominadas *privacy-enhancing technologies* (PET) (Holvast 2007, 738).

Los artistas, por su parte, se han posicionado políticamente y han intentado con sus obras promover un discurso crítico respecto de la vigilancia ostensiva. Se pueden verificar dos estrategias para resistir y combatir la sociedad de la vigilancia. La primera de estas es llamar la atención sobre el problema (que no siempre es notado por el usuario común) e instigar el público a exigir la preservación de su derecho a la privacidad. La segunda "táctica" es la *sousveillance*, comentada en el proyecto de Hasan Elahi, es decir, ofrecer y exigir visibilidad, transparencia, total a todo y a todos, incluso, y especialmente, a los Gobiernos y a las empresas.

En general, sin embargo, tras el análisis de las obras en la propuesta estética del arte de la vigilancia, se observa que la mayoría de los artistas actúan exponiendo las tecnologías de la vigilancia. Así, los procedimientos de vigilancia visibles (pero, para muchos, desapercibidos) e invisibles se hacen transparentes para el público. A grandes rasgos, podríamos afirmar que los artistas utilizan las tecnologías de vigilancia de forma activa y pasiva. La forma pasiva sería simplemente mostrar que la vigilancia existe, aunque no siempre se note. La figura 6, del artista británico Banksy, expone precisamente la existencia de una cámara de vigilancia en la pared exterior de un banco de Londres. Resulta interesante que el simple hecho de que el artista escriba una frase hace que los transeúntes se fijen en la cámara que, quizá, sin esta provocación, no se notaría.

La vía activa, por otro lado, sería precisamente el uso de las tecnologías en la obra de arte con la intención no solo de hacerlas visibles, sino como forma de promover un diálogo crítico y

sensible entre artista y público. A veces, esta visibilidad es más explícita, como en la que un hacktivista critica abiertamente al presidente Barack Obama, parodiando su famoso eslogan de campaña "Yes, we can!" quien lo modifica a "Yes we scan", y así expone los procedimientos de vigilancia aún vigentes en su Gobierno. El hacker reemplazó la figura original del teléfono Galax Android que ofrecía a los compradores una aplicación para descargar canciones del álbum *Magna Carta Holy Grail* del rapero Jay-Z (2013). La aplicación fue clonada por el hacker y funcionaba bien, hasta que en una fecha estratégica (4 de julio, Día de la Independencia de los Estados Unidos) cambió la imagen por la del presidente Obama. La crítica implícita en este procedimiento, que hacía uso de la propia tecnología de espionaje del Gobierno estadounidense, es que los ciudadanos deben liberarse (independizarse) de la vigilancia omnipresente impuesta por el Gobierno.

Si el hacktivismo incluso se consideró una actitud criminal, como lo demostró los casos de Julian Assange o WikiLeaks, hoy día esta actitud está incrustada en las prácticas digitales (Gorham 2023). En el ámbito artístico, existen festivales que fomentan el hacktivismo como HACK.Fem.EAST (creado por muchos artistas y activistas que trabajan en redes digitales en Europa del Este; véase https://hackfemeast.org/web/), que desde 2008 une el activismo *online* con las cuestiones de género contemporáneas.

Algunos artivistas no solo se niegan a condonar estas tecnologías, sino que también desafían los métodos de vigilancia impuestos, como los pasaportes biométricos y el chip RFID. El proyecto Border Xing, realizado en 2000 por Heath Bunting y con Kayle Brandon, es uno de estos tipos activos de artivismo. Bunting pasó siete meses cruzando ilegalmente las fronteras de Europa a pie, documentó y luego publicó el proceso completo como manual. Enumeró el equipo necesario, las herramientas, las fuentes de alimentos y ayuda, así como las dificultades esperadas. Solo se puede tener acceso a Border Xing desde una IP fuera de la Unión Europea (UE). Con esta experiencia radical, los autores crean su propia microbase de datos accesible, que funciona en oposición a las oficiales.

Sin embargo, el artivismo digital presenta también trabajos en los que la invasión de la privacidad es más sutil, pero sin dejar de ser perturbadores, como los ejemplificados en las propuestas de Dewey-Hagborg (figura 3) y David Rokeby (figura 4). Ambos artistas, a su manera, critican activamente la invasión de la privacidad impuesta en la sociedad de la vigilancia. Dewey-Hagborg llama la atención sobre el problema de la vigilancia forense actuando como alguien que invade el derecho a la privacidad. Al recoger (sin permiso) muestras de "residuos" dejados por las personas, obliga al público a indignarse con este procedimiento, ya que las máscaras creadas a partir del ADN resultante de las muestras recogidas podrían mostrar el rostro de cualquier persona. Esto llevaría al espectador a preguntarse: "¡Yo no autoricé eso!", y así se establece el problema de la invasión de la privacidad. Rokeby, por su parte, graba imágenes de transeúntes sin contar con su permiso. Esto también podría llevar a cuestionar la necesidad de la respectiva autorización de los filmados para ser utilizados en una obra de arte, lo que a su vez haría avanzar el debate sobre los distintos niveles y las capas de invasión, ya que, si las agencias gubernamentales pueden grabar imágenes sin autorización, ¿por qué no podría hacerlo también el artista?

El análisis de las obras creadas por los artistas en el orbe de la *sousveillance art* muestra una actitud de combate y resistencia ante el peligro que impone la sociedad de la vigilancia, es decir, el peligro de que la vigilancia se asimile tanto al paisaje cotidiano que deje de percibirse. Este aspecto llevaría precisamente a la pérdida de individualidad causada por el conformismo de los ciudadanos a la sociedad de la vigilancia. Los artistas del arte de la vigilancia tienen el mérito de actuar de forma crítica, problematizando y obligando al público a sacar la cabeza del suelo y a ejercer el derecho a la ciudadanía.

▪ CUAD. MÚSIC. ARTES VIS. ARTES ESCÉN. ▪ VOL. 18 - 2 ▪ PP. 218 ▪ JULIO - DICIEMBRE 2023 ▪ BOGOTÁ, D.C., (COLOMBIA) ▪ ISSN 1794-6670 ▪

[NOTAS]

1. Este artículo amplía y profundiza algunos temas analizados en Corrêa y Alves (2022).
2. Exposición realizada de febrero a agosto de 2017 en el Museo de Fotografía de Berlín, comisariada por Stuart Alexander, Susan Meiselas y Yukiko Yamagata. Organizado por Open Society Foundations (Nueva York) en cooperación con Kunstbibliothek, Staatliche Museen de Berlín.
3. El término sousveillance, acuñado por Steve Mann, proviene de las palabras francesas contrastantes sur, que significa "arriba", y sous, que significa "abajo", es decir, "vigilancia" denota el "ojo en el cielo" que mira desde arriba, mientras sousveillance denota traer la cámara u otros medios de observación al nivel humano, física (montar cámaras en personas en lugar de edificios) o jerárquicamente (personas comunes que observan, en lugar de autoridades superiores o arquitecturas que observan) ("Sousveillance" 2023).
4. Según David Owen, en 1918, los militares estadounidenses se dieron cuenta de que sus conversaciones telefónicas eran escuchadas. Para evitar que los espías entendieran lo que se decía, pusieron a los indios a hablar en su lengua materna, y así transmitir los contenidos más importantes y secretos (Owen 2002).

[REFERENCIAS]

Barreto, Wanderlei de Paula y Luciany Michelli Pereira dos Santos. 2006. "O conceito aberto de desdobramento da personalidade e os seus elementos constitutivos nas situações de mobbing ou assédio moral". *Revista Jurídica Cesumar-Mestrado* 6, n.º 1: 473-487. https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/322/181

Beniger, James R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press.

Bruno, Fernanda, Paola Barreto y Milena Szafir. 2012. "Surveillance Aesthetics in Latin America: Work in progress". *Surveillance & Society* 10, n.º 1: 83-89. https://doi.org/10.24908/ss.v10i1.4212

"Blue Sky Days". 2013. Tomas van Houtryve. https://tomasvh.com/works/blue-sky-days/

Dewey-Hagborg, Heather. 2023. "Sci-Fi Crime Drama With a Strong Black Lead". https://thenewinquiry.com/sci-fi-crime-drama-with-a-strong-black-lead/

Corrêa, Antenor Ferreira y Lorena Ferreira Alves. 2022. "Sociedade de vigilância: Manifestações artísticas em meio ao descarte da privacidade". *ARS* 20, n.º 46: 441-491. https://doi.org/10.11606/issn.2178-0447.ars.2022.167047

Gorham, Shley. 2023. "The Political Meaning of Hacktivism". https://limn.it/articles/the-political-meaning-of-hacktivism/

Holvast, Jan. 2007. "History of Privacy". En *The History of Information Security: A Comprehensive Handbook*, editado por Karl de Leeuw and Jan Bergstra, 737-769. Amsterdam: Elsevier.

"Interactive Installations: Sorting Daemon (2003)". 2013. Davidrokeby. http://www.davidrokeby.com/sorting.html

Jonas, Jeffrey. 2015. "The Surveillance Society and the Transparent You". En *Privacy in the Modern Age-The Search for Solutions*, editado por Marc Rotenberg, Julia Horwitz y Jeramie Scott. Nueva York: New Press.

Lacaze, Laura Mabel. 2016. "Vigilância masiva de comunicaciones: Una (ciber)inquisición". En *Anais IV Simpósio Internacional Lavits: ¿Nuevos paradigmas de vigilancia? Miradas desde América Latina*, editado por Pablo Rodriguez, Laura Siri, Camilo Rios Rozo y Fernanda Bruno. Buenos Aires: Lavits. https://lavits.org/es/anais-2016/

Lyon, David. 2010. "Surveillance, Power and Everyday Life". En *Emerging Digital Spaces in Contemporary Society: Properties of Technology*, editado por Phillip Kalantzis-Cope y Karim Gherab-Martín, 107-120. Londres: Palgrave Macmillan.

McDougall, Bonnie S. y Anders Hansson. 2002. *Chinese Concepts of Privacy*. Köln: Brill.

Owen, David. 2002. *Hidden Secrets: The Complete History of Espionage and the Technology Used to Support It*. Ontario: Firefly Books.

Museum für Fotografie. 2017. "Watching You, Watching Me. A Photographic Response to Surveillance". https://www.smb.museum/en/museums-institutions/museum-fuer-fotografie/exhibitions/detail/watching-you-watching-me-a-photographic-response-to-surveillance/

Patriot Act. 2017. *History.com*, 19 de diciembre. https://www.history.com/topics/21st-century/patriot-act

Pariser, Eli. 2012. *O Filtro Invisível: O que a internet está escondendo de você*. São Paulo: Zahar.

Rengel, Alexandra. 2013. *Privacy in the 21st Century*. Leiden: Martinus Nijhoff Publishers.

"Sousveillance". 2023. Wikipedia. https://en.wikipedia.org/wiki/Sousveillance

"Surveillance society". 2023. Collins. https://www.collinsdictionary.com/dictionary/english/surveillance-society

"Stranger Visions". 2009-2023. Heather Dewey-Hagborg. https://deweyhagborg.com/projects/stranger-visions

Vieira, Waleska Duque Estrada. 2016. "A privacidade no ambiente cibernético: Direito fundamental do usuario". Tesis de grado. Universidade Estadual do Ceará.