Teknokultura. Revista de Cultura Digital y Movimientos Sociales
ISSNe: 1549-2230

EDICIONES COMPLUTENSE

https://doi.org/10.5209/tekn.80980

Ofuscación. Tácticas de resistencia frente al capitalismo de vigilancia

Fátima Solera Navarro[1]

Recibido: 14 de marzo de 2022 / Aceptado: 15 de septiembre de 2022 / **OPR**

Resumen. Aunque la vigilancia masiva no es algo exclusivo de Internet, actualmente el nivel de recopilación de datos que realizan las agencias gubernamentales y las corporaciones nos interpela a diversos niveles. En unas circunstancias donde la abstinencia digital no es una opción válida para gran parte de la población, y donde la recopilación de datos es una condición inherente a muchas actividades sociales esenciales, este artículo tiene como objetivo realizar una revisión teórica de una de las tácticas de resistencia críticas al actual régimen de vigilancia digital: la ofuscación.
Palabras clave: datificación; hacking; privacidad; tecnologías expresivas; vigilancia digital.

[en] Obfuscation. Tactics of resistance against surveillance capitalism

Abstract. Although massive surveillance is not exclusive to the Internet, the current volume of data collection and preservation by government agencies and corporations confronts us with noxious consequences on different levels. In an information context where the digital abstinence is not a valid option for most people, since data collection is an inherent condition for many essential social activities, we present a theoretical review of a critical re-sistance tactic to this daily digital surveillance regime: the obfuscation.
Keywords: datafication; digital surveillance; expressive technologies: hacking; privacy.

Cómo citar: Solera Navarro, F. (2023). Ofuscación. Tácticas de resistencia frente al capitalismo de vigilancia. *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, *20*(1). 125-131. https://doi.org/10.5209/tekn.80980

1. Introducción: la toxicidad en la red

La 'ofuscación' es un concepto bastante trabajado en la literatura anglosajona, pero escasamente investigado fuera de este ámbito. Nuestro propósito en este texto es una demarcación de este concepto a partir de una revisión teórica. No obstante, para comenzar delineando en qué consiste la ofuscación, primero es necesario entender cómo funciona el régimen actual de recopilación y conservación de datos personales y qué papel ocupan las corporaciones y agencias gubernamentales, dentro de lo que Zuboff (2020) denomina el 'capitalismo de vigilancia'.

Brunton y Nissembaun (2015) definen la ofuscación como el conjunto de «herramientas de producción, inclusión, suma o comunicación de datos engañosos, ambiguos o falsos en un esfuerzo por evadir, distraer o confundir a los recopiladores de datos o devaluar la confianza (y el valor) de las bases de datos que generan» (párr. 1). Además de todos los contaminantes de nuestra era, convivimos con otro material tóxico que es manipulado y almacenado constantemente. Hablamos de los datos personales, definidos, según la Comisión Europea, como:

> Cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal. Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales (s.f., párr. 1).

Comencemos primero con la toxicidad más física, la que a menudo se camufla bajo el eufemismo de la 'nube'. Esta referencia remite a espacios más livianos y limpios, incluso volátiles, donde se oculta la materialidad del hardware necesaria para que la nube funcione, es decir, los dispositivos, aparatos y cables que sustentan cualquier tipo de tecnología. Esta imagen de una 'nube esponjosa' es engañosa. Detrás del relato construido en torno a ella no hay más que una

[1] Universidad de Málaga (España)
E-mail: fsolera@protonmail.com
ORCID: https://orcid.org/0000-0003-0143-7629

computadora grande, potente y centralizada. Como señala Snowden (2019, p. 265):

> Ya no importa en realidad qué tipo de ordenador personal tengas, porque los auténticos ordenadores de los que dependemos están en los enormes centros de datos que las empresas basadas en la nube construyeron en todo el mundo. [...] Como resultado, tus datos ya no son tuyos de verdad. [...] No hay ninguna propiedad menos protegida, y pese a ello ninguna propiedad es más privada.

Gracias a la web CloudMap de la consultora Telegeography, sabemos que los centros de datos están controlados principalmente por seis empresas, entre las que destacan Amazon Web Services, Microsoft Azure, Google Cloud y Ali Baba, siendo esta última la única que no es de origen estadounidense. Este conglomerado 'gaseoso' se asemeja a las reservas de gas natural del subsuelo, hoy tan disputadas en la geopolítica mundial. Como señalan Perragin y Renouard (2021), «las comunicaciones, los flujos financieros y el acceso a los datos almacenados en la 'nube' dependen de los cables submarinos» (párr. 9). De hecho, si visitamos la web Submarinecablemap.com, también de la consultora Telegeopraphy, vemos como el control y construcción de estos particulares 'gaseoductos' digitales también corre a cargo de las mismas empresas que controlan los centros de datos. Estas empresas conforman lo que se conoce como un oligopolio digital, puesto que ostentan la propiedad exclusiva de estos cables. De este modo, como constata Broca (2020), «la economía digital no es ni 'inmaterial' ni 'verde'» (párr. 1). Este autor recuerda que el principal centro de datos de Amazon, situado en Virginia, adquiere la mayor parte de su electricidad del carbón, y que tres de las seis empresas que controlan la nube colaboran con las grandes petroleras para optimizar la localización y explotación de sus yacimientos petrolíferos. De hecho, la industria digital consume entre un 1% y 3% del total de la electricidad mundial, triplicando la huella de carbono de países como Francia o Reino Unido (Pitron, 2021).

El efecto contaminante de la recopilación y la conservación de datos no sólo tiene lugar en el plano material: su toxicidad se expande al mundo de las ideas. Los datos personales son un material muy sensible y codiciado. Como advierte Véliz (2021, p. 110), «cuanto más tiempo tengan almacenados nuestros datos y cuanto más los analicen, más probable resultará que acaben usándolos contra nosotros». Este tipo de afirmaciones no provienen de la literatura de ficción, sino de aprendizajes del pasado. Por ejemplo, la decisión de señalar la religión de cada persona en los censos de población que se elaboraron en Holanda antes de la Segunda Guerra Mundial tuvo consecuencias fatales para los judíos de este país cuando llegaron a conocimiento del ejército nazi. Por su parte Schwartz (1989), décadas antes del escándalo de Cambridge Analytica, advertía del peligro para la democracia de no estructurar correctamente el uso social de la información.

Las empresas dedicadas a la minería datos buscan conocer de la forma más exhaustiva posible nuestros comportamientos. Por tanto, es conveniente ubicar la minería de datos digital como una parte del 'Capitaloceno' al que alude Haraway (2019) dentro de su reflexión sobre los tiempos turbios y problemáticos que vivimos. A diferencia del 'Antropoceno', que repara en la capacidad de actividad humana en devenir en una fuerza ambiental destructiva a nivel mundial, el concepto de Capitaloceno consideran que esta potencia destructiva proviene más de la organización capitalista que de la actividad humana en abstracto (García y Jiménez, 2020). Haraway (2019, p. 19) considera que, en lugar de esperar que una tecnología futura, todavía no pensada, nos salvará, o que podemos dar el juego por perdido, «nuestra tarea es generar problemas, suscitar respuestas potentes a acontecimientos devastadores, aquietar aguas turbulentas y reconstruir lugares tranquilos».

Las tácticas de ofuscación que presento en este texto buscan encarar colectivamente el problema hasta aquí descrito, proteger(nos) mediante la "sobreexposición" en la red y, en muchos casos, simplemente buscan ganar tiempo mientras la reivindicación legislativa sobre este problema llega a buen puerto. Todas estas prácticas tienen también una función expresiva, ya que, en términos de Haraway (2019, p. 23), desafían la idea de que las cosas «realmente importan solo si funcionan. O, peor, que algo importa solo si lo que yo y mis colegas expertos hacemos funciona para arreglar las cosas».

3. La privacidad es un asunto colectivo

La vigilancia masiva no es algo exclusivo de Internet. El poder llega hasta donde alcanza la tecnología; con el avance de ésta, su mirada se ha ido ampliando. Si durante largo tiempo ser observado y que se llevase un registro de nuestra vida era considerado un privilegio, según Foucault (1988, p. 196) «los procedimientos disciplinarios invierten esa relación, rebajan el umbral de la individualidad descriptible y hacen de esa descripción un medio de control y un método de dominación».

Lo que quizá sí es inherente a la tecnología es el surgimiento de empresas cuyo beneficio reside principalmente en la acumulación de nuestros datos personales a través de la vigilancia. Siguiendo métodos similares a los del capitalismo industrial, actualmente nuestro comportamiento se transforma en mercancía otorgando a empresas y agencias gubernamentales un nuevo poder: predecir e influir en nuestra conducta. Este modelo de capitalismo, conocido como el capitalismo de vigilancia, emerge directamente de la información que obtienen sobre nosotros.

Sin embargo, este poder no se presenta ante nosotros con una violencia explícita a la que debamos

sucumbir irremediablemente. En su lugar, ha ido creciendo lentamente, impidiendo que la mayoría de nosotros optemos por alguna de las alternativas existentes. Tal y como explica Zuboff (2020), es importante entender que, para compañías como Google o Facebook los usuarios no somos el producto, sino una fuente de materia prima con la que trabajan.

La autora también recalca que el problema no es que las personas reciban una compensación económica por la cesión de esta 'materia prima'. De hecho, los sistemas de precios compensatorios solo contribuirían a legitimar «la extracción de la conducta humana para su fabricación y venta» (Zuboff, 2020, p. 134). Por su parte Rimbert (2018), atendiendo a la monetización individualista de la privacidad, apunta que estos datos no son útiles de manera individual, sino que su validez reside en su agrupación y tratamiento estadístico. Por tanto, si el valor de estos datos radica en su carácter colectivo, sería más lógico socializarlos en lugar de insistir en su propiedad individual.

Actualmente, estamos en una situación en la que nuestro estilo de vida nos aboca a pasar cada vez más tiempo dentro de la red. En este espacio es verdaderamente difícil eludir los sistemas de recopilación de datos y su vigilancia. Así el concepto de 'públicos en red' al que alude Zuboff (2020) resulta paradójico, pues estamos cada vez más expuestos, no solo por la naturaleza pública de dichos espacios, sino porque la mayoría de ellos pertenecen a empresas privadas. El traslado de parte de nuestra vida al mundo digital no hace sino complicar más la posibilidad de interactuar constructivamente, especialmente en un entorno que todavía podemos considerar offline. Como afirma Peirano (2019) la fragilidad del tejido social dificulta la cooperación y la resolución de problemas colectivos se vuelve más complicada.

En definitiva, es posible entender la dimensión colectiva de la privacidad en dos sentidos: por un lado, la exposición de los datos personales puede vulnerar el derecho a la privacidad de otras, dado que vivimos conectados los unos a los otros por multitud de vínculos (laborales, sociales y, por supuesto, genéticos) y en el sentido que «las pérdidas de privacidad se sufren a escala colectiva» (Véliz, 2021, p. 95). Por lo tanto, es importante remarcar la importancia de la dimensión colectiva para la protección de la privacidad.

4. Gases de escape digitales

«Navegar es una actividad promiscua». Con esta afirmación Peirano (2015, p. 25) evidencia que cuando realizamos cualquier acción desde nuestro navegador –como pinchar un enlace o buscar un término en Google–, éste intercambia «fluidos digitales con otros ordenadores desconocidos, adentrándose en una jungla de servidores y proveedores de servicios que pueden estar en cualquier parte del mundo y que obedecen a diversas legislaciones».

Del mismo modo, cuando tecleamos estamos generando un texto que, a su vez, crea un relato, a veces inconexo, a veces contradictorio, pero siempre nuestro. Es un escrito que está a la vista del público y sobre el que nosotros respondemos. Un ejemplo son nuestras publicaciones en redes sociales, nuestras aportaciones en los comentarios de algún blog o nuestra propia página web. Pero este texto no es lo único que queda escrito: cuando tecleamos en Internet o utilizamos cualquier dispositivo conectado a él, le acompaña lo que Zuboff (2020, p. 256) denomina un «texto en la sombra» que «se alimenta automáticamente de nuestra experiencia incluso cuando nosotros no hacemos otra cosa que cumplir con las rutinas normales y necesarias de la participación social». De este modo, nuestras aportaciones al primer texto, aquello que se nos ha hecho creer que era el simple resultado de nuestra actividad, se transforma en materia prima para la extracción del segundo texto, que permanece oculto y se va acumulando con fines mercantilistas hasta ofrecer más información sobre nosotros de la que somos conscientes.

Adicionalmente, al igual que nuestro relato está acompañado de las expresiones de nuestra cara o la posición de nuestro cuerpo, nuestra actividad en la red está acompañada de otros gestos digitales. Para designar a esta multiplicidad de signos añadidos a la escritura, estimo que el término más acorde es el de 'metadatos':

> El prefijo de este término, meta-, que tradicionalmente se traduce como 'por encima' o 'más allá', se utiliza aquí en el sentido de 'acerca de': los metadatos son datos acerca de datos. Siendo más precisos, son datos que están hechos de datos: un grupo de etiquetas y marcadores que permiten que los datos sean útiles (Snowden, 2019, p. 246).

Una forma de entender los metadatos es definirlos como los 'registros de actividad' que realizan nuestros dispositivos: la hora a la que realizas una llamada, a quién y cuánto dura, o cuánto tiempo estamos viendo la televisión. Igualmente, este concepto abarca todo aquello que hacen nuestros dispositivos de forma mecánica: contar los pasos que damos, ubicar nuestra geolocalización o detectar nuestros latidos mientras dormimos. Estos hechos por si solos pueden llegar a parecer inocuos, pero debemos tener en cuenta que los metadatos se generan de manera automática, por lo que apenas tenemos control sobre ellos. Son las máquinas las que se encargan de crearlos, recopilarlos y analizarlos. Como señala Snowden (2019, p. 247), «nuestros dispositivos están constantemente emitiendo comunicaciones en nuestro nombre, queramos o no».

Todo esto va más allá de la posición de nuestro cuerpo en un tiempo y lugar determinado. Como advierte Zuboff (2020, p. 393), las «máquinas y los al-

goritmos deciden lo que quieren decir mi respiración y mis ojos, mis maxilares, ese nudo en la garganta o los signos de admiración que mostré con toda inocencia y esperanza».

Las corporaciones y agencias de seguridad gubernamentales que tienen acceso a este tipo de textos, además de utilizarlos para crear perfiles y categorizarnos según nuestro comportamiento, o simplemente vigilarnos, también los emplean para distorsionar la visión del mundo y adecuarlo a sus intereses (Pasquale, 2015). Esta capacidad corrobora las asimetrías de poder y epistémica, a las que aluden Brunton y Nissenbaum (2011, párr. 12-16) sobre la recopilación, agregación y minería de datos digitalizadas:

> Primero, la asimetría de poder: rara vez podemos escoger si somos o no controlados, qué pasa con la información sobre nosotros y qué nos pasa a nosotros debido a ella. [...] Segunda, e igualmente importante, es la asimetría epistémica: a menudo no somos plenamente conscientes del control, y no sabemos lo que será de la información producida por dicho control, ni dónde acabará ni lo que puede hacerse con ella. [...] En cuanto personas cuyos datos son recopilados, lo que sabemos de la situación es problemático, y lo que no sabemos es sustancial.

Convencida de la ineficacia y la imposibilidad de que tenga lugar la 'abstinencia digital' en nuestras sociedades, estimo urgente poner en conocimiento las posibles alternativas con las que podemos contar para proteger nuestra privacidad de manera colectiva, así como mostrar nuestra disconformidad o presencia crítica.

5. Ofuscación. Generar ruido para vencer a la vigilancia

Lessig (2009) estudia la privacidad desde el lado de la simplicidad técnica. En su trabajo, el autor explica lo fácil que es difundir copias perfectas de obras intelectuales. Para ello, hace referencia a cuatro reguladores que permiten al Estado y las corporaciones rastrear nuestra huella digital: las leyes, las normas sociales, los mercados y las arquitecturas tecnológicas.

En primer lugar, la ley no impone a los monopolios fuertes medidas de protección de datos. Hay que recordar que el actual Reglamento General de Protección de Datos (RGPD) no entró en vigor hasta 2018, tras las filtraciones de Snowden y la victoria judicial de Max Schrems contra el acuerdo de *safe harbour* entre la UE y EE. UU. (Peirano, 2019, p. 105-110). Para O'Neil (2017), estas leyes son la artillería pesada en materia de privacidad, puesto que obligan a las empresas y administraciones a solicitar nuestro consentimiento antes de utilizar nuestros datos, lo que ilegaliza su venta. Para O'Neil (2017, p. 264) «esto evita que los datos acaben en manos de las agencias cuyos expedientes alimentan las calificaciones electrónicas tóxicas y las campañas de microsegmentación».

En segundo lugar, en lo que respecta a las normas sociales y el mercado, cabe destacar que existen fundaciones y empresas cuyo objetivo es concienciar a la ciudadanía sobre el derecho a la privacidad (sin ellos el RGPD no hubiese tenido cabida). Sin embargo, este tipo de entidades defienden la autorregulación mercantil, situándonos como los únicos responsables de proteger nuestros datos.

Por último, nos encontramos con las arquitecturas tecnológicas, donde «el código es ley» (Lessig, 2009, p. 31). Las cajas negras guardan diversas asimetrías de poder a las cuales no podemos tener acceso puesto que, además, están protegidas por las legislaciones sobre privacidad. De ahí el fracaso de protocolos voluntarios de exclusión del seguimiento como el P3P –diseñado para que los diferentes sitios web declaren los motivos y posibles usos por los que recopilan la información de sus usuarios, y asegurar un mayor control de su información personal– (Lessig, 2009, p. 363-364) o el *Do Not Track* que, siendo técnicamente impecables, para su puesta en práctica necesitaban que las corporaciones, poco dispuestas a renunciar a la materia prima de su extractivista modelo de negocio, los incorporasen.

Aquí es donde emergen los diferentes instrumentos de ofuscación, que persiguen tres metas relacionadas entre sí:

- Protección: alude a la acción directa para conseguir minimizar el perjuicio de la falta de privacidad.
- Expresión: amplifica las perspectivas sociales, culturales o políticas (Howe, 2015, p. 93).
- Subversión: referida al grado en que la herramienta intenta quebrantar el sistema contra el que actúa.

Estimo que la ofuscación puede entenderse como táctica si recuperamos las claves que de Certeau (1990) ofrece con su caracterización de los 'modos de hacer'. Con este término, el historiador francés engloba las prácticas de consumo que, pese a trabajar «con un vocabulario y una sintaxis recibidos», revelan una «invención de lo cotidiano» (de Certeau, 1990, p. 38). La caracterización formal de dicha invención remite a dos ejes teóricos. Por un lado, a las combinaciones operativas que, en clave de uso, se ponen en marcha en estas prácticas; y de otra, la perspectiva 'polemológica' que da cuenta de «las operaciones casi microbianas que proliferan en el interior de las estructuras tecnocráticas, cuyo funcionamiento desvían mediante una multitud de 'tácticas' articuladas sobre los 'detalles' de lo cotidiano» (de Certeau, 1990, p. XL).

Debemos entender la táctica como un cálculo de fuerzas de aquellos que se encuentran en una situación de ausencia de poder y, por lo tanto, no pueden eludir la 'vigilancia panóptica'. De Certeau (1990, p. 46) entiende este proceso como:

> Un estilo de intercambios sociales, un estilo de invenciones técnicas y un estilo de resistencia moral, es decir, una economía del 'don' (generosidades *à charge de revanche*), una estética de 'golpes' (operaciones de artistas) y una ética de la tenacidad (mil maneras de negarle al orden establecido el estatuto de ley, de sentido o de fatalidad).

Esta caracterización táctica de la ofuscación concuerda con la siguiente definición que plantean Brunton y Nissenbaum (2015, p.79):

> A la gente que no es rica o políticamente influyente y que no está en posición de rechazar las condiciones de participación [...] la ofuscación le ofrece cierto grado de resistencia, oscuridad y dignidad, cuando no una reconfiguración permanente del control o una inversión de la jerarquía arraigada.

Es este cariz táctico de la ofuscación el que acaba marcando la diferencia de lo que

Brunton y Nissenbaum (2011) definen como una 'resistencia vernácula' frente a otras formas de protección de la privacidad. Junto a ello, estos autores explican los diversos motivos por los que se puede hacer uso de estas tácticas. Entre ellos se encuentran: (1) el deseo de defenderse de los peligros de la recopilación de datos, (2) la acción contra la asimetría de poder y conocimiento, y (3) la ocultación de actividades legítimas o ilegítimas para hacer que el sistema de recopilación de datos sea inservible (Brunton y Nissenbaum, 2015). A continuación vamos a presentar la clasificación que realizan de cuatro tipos ideales de ofuscación, las cuales pueden llegar a combinarse (Brunton y Nissenbaum, 2011, párr. 29-50).

5.1. Ofuscación con limitaciones temporales

El primer tipo de ofuscación engloba las denominadas 'estrategias de señuelo'. Estas estrategias se activan cuando es inevitable estar expuesto a la recopilación de datos, puesto que ayudan a ganar tiempo para el desarrollo de otras acciones.

Para entender esta modalidad siempre se utiliza el ejemplo de los pilotos Aliados que sobrevolaron Hamburgo durante la Segunda Guerra Mundial. En este caso, era imposible evitar ser vistos por los radares enemigos, por lo que les confundieron lanzando bolas de papel de aluminio. Este acto conseguía desconcertar al radar enemigo impidiendo saber realmente si lo que mostraba la pantalla era un objetivo o no. Este tipo de tácticas de ofuscación no son exclusivas del ámbito digital, pero pueden aplicarse a estos entornos (Brunton y Nissembaun, 2015, p. 88).

5.2. Ofuscación cooperativa

La ofuscación cooperativa hace referencia a las prácticas que se realizan de manera colectiva para generar confusión. Cuantas más personas colaboran, más efectiva es la estrategia.

Como mencioné previamente, antes de que el capitalismo de la vigilancia tomase su forma actual, también se desarrollaron acciones de recopilación de datos. Por ejemplo, las cadenas de supermercados utilizaban tarjetas de fidelización de sus usuarios, las cuales ofrecen ciertas ventajas a sus usuarios a cambio de registrar los hábitos de compra que realizan en sus establecimientos. Frente a este tipo de individualización de los perfiles surgieron diversos grupos coordinados que se intercambiaban las tarjetas personales (Brunton y Nissenbaum, 2015).

Otro ejemplo lo encontramos en la criptografía, que consiste en la protección de la información a través del uso de códigos, puede entenderse estrictamente como una ofuscación de datos (y metadatos), que se esconden entre capas de ruido matemático. Este tipo de movimientos representan una estrategia de ofuscación colectiva, puesto que la criptografía se vuelve más efectiva cuanto más la usamos los ciudadanos con normalidad, ya que complica a las corporaciones la tarea de identificar los intercambios triviales de la información relevante. Lo mismo sucede con Tor, el sistema de encaminamiento de cebolla «cuya función de desagregación y camuflaje criptográficos de la identidad y actividad del tráfico web se vuelve más rápida y segura cuanta más gente lo adopta, más aún si entre ella surgen nuevos nodos de salida de la red» (Cabello y Solera, 2020, p. 343).

5.3. Ofuscación selectiva

Este tipo de ofuscación se utiliza para ocultar datos a adversarios específicos. Aquí destaca la pionera TrackMeNot, una extensión libre de los navegadores Mozilla Firefox y Google Chrome que funciona mediante la automatización de 'consultas fantasma': es decir, la aplicación realiza progresivamente consultas que no son reales, permitiendo que los usuarios puedan camuflar sus verdaderos intereses (Howe y Nissenbaum, 2009).

Un ejemplo más reciente lo encontramos en el dispositivo Fangø, desarrollado por Martín Nadal (s.f.) dentro del programa European Media Artist in Residence Exchange de la European Media Art Platform (EMAP/EMARE). Este dispositivo consiste en un cargador de móvil que ejecuta de manera aleatoria consultas en Google, Amazon y otros buscadores. El objetivo principal de este proyecto es agregar ruido a los datos capturados y engañar a estos sistemas en su proceso de captura de datos, dificultando así sus predicciones y devaluando su valor.

5.4. Ofuscación por ambigüedad

Esta opción consiste en hacer inservibles las fuentes de datos personales. Destacaríamos aquí otra extensión libre de Firefox, Chrome y Opera: AdNauseam. Esta extensión, además de bloquear los anuncios para

el usuario, hace *click* en cada uno de ellos con el objetivo de hacer inservible la segmentación publicitaria para el servidor.

Otro ejemplo es el proyecto Adversarial Fashion creado por la *hacker* y diseñadora de moda Kate Rose. En este proyecto Rose, estampa imágenes de matrículas de coches en la ropa que diseña, logrando confundir a los lectores automatizados. Con esta idea la diseñadora denuncia el aumento de sistemas de videovigilancia y el hecho de que una buena parte de ellos no están supervisados por humanos, ilustrando a su vez cómo nuestro propio cuerpo puede funcionar como una herramienta para ofuscar los sistemas de vigilancia digital.

6. Conclusiones

Aunque los ejemplos que se han expuesto en este artículo para explicar la ofuscación son diferentes, podemos identificar ciertos elementos comunes a todos ellos. Por un lado, todas estas prácticas se posicionan críticamente contra la recopilación masiva de datos que posibilita el actual procesamiento algorítmico, y todas se dirigen hacia los sistemas algorítmicos, buscando sus puntos ciegos para contrarrestar su impacto. Por el otro, estos sistemas reivindican aquello que los algoritmos menos aprecian de nosotros, como señala Sabariego (2020), «somos: impredecibles, diferentes, erráticos, tendentes al equívoco, ambiguos. [El interés de los algoritmos] radica en [...] igualarnos en el trazo grueso a través del consumo de nosotros mismos» (p. 1).

Hay que enfatizar que la ofuscación remite a tácticas que, en su mayoría, buscan generar ruido de fondo sobre nuestra actividad para distorsionarla. De hecho, en la mayoría de los casos estas prácticas ni siquiera alteran nuestra percepción de lo que estamos viendo/consumiendo. Por ejemplo, para ver el ruido que genera AdNauseam hay que acceder a la extensión; de lo contrario, solo se percibe como un bloqueador de anuncios más. Por su parte, la obra de Kate Rose a primera vista puede ser sólo una sudadera con estampado de matrículas.

Estos tipos de resistencias tácticas a la automatización de nuestros datos sugieren su categorización como tecnologías expresivas. La realidad generada por la ofuscación sería, en palabras de Howe (2015, p. 93), «una automatización táctica tan limitada en alcance y contexto que su objetivo final es a menudo eliminar la necesidad de sí mismo». Por último, quiero señalar que estas herramientas no debieran reemplazar otros modos de defensa de la privacidad, como la implementación leyes, normas sociales o asegurar la privacidad de los usuarios desde el diseño de las herramientas o por defecto. Más bien podrían entenderse como un complemento a las mismas, sin renunciar a perseguir la misma finalidad expresiva de la ofuscación por otros medios.

7. Referencias

Adversarial Fashion (s.f.). *DEFCON 27 Crypto & privacy presentation*. https://adversarialfashion.com/

Broca, S. (2020, marzo). La tecnología digital funciona con. *Le Monde Diplomatique en español*. https://mondiplo.com/la-tecnologia-digital-funciona-con-carbon

Brunton, F. y Nissenbaum, H. (2011, 2 de mayo). Vernacular resistance to data collection and analysys: A political theory of obfuscation. *First Monday*, *16*(5). https://firstmonday.org/article/view/3493/2955

Brunton, F. y Nissenbaum, H. (2015). *Obfuscation*. The MIT Press.

Cabello, F. y Solera, F. (2020). Ofuscación algorítmica. En J. Sabariego, A. Jobim y F. Baldissera (eds.). *Algoritarismos*. Tirant Lo Blanch. 332-346.

Certeau, M. de (1990). *L'Invention du quotidien, vol. 1. Arts de faire.* Gallimard.

Cloud Map (s.f.). *TeleGeography. Cloud infraestructure map*. *Cloudinfraestructuremap.com*. https://www.cloudinfrastructuremap.com/

Comisión Europea (s.f.). *¿Qué son los datos personales?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

Foucault, M. (1988). *Vigilar y castigar: Nacimiento de la prisión* (15a ed. en castellano, 6a ed. de España). Siglo XXI de España.

García Barrios, R. y Jiménez Martínez, N. (2020, 13 de julio). ¿Antropoceno o capitaloceno? *Nexos.* https://medioambiente.nexos.com.mx/antropoceno-o-capitaloceno/

Haraway, D. J. (2019). *Seguir con el problema. Generar parentesco en elChthuluceno.* Consonni.

Howe, D. C. (2015). Surveillance countermeasures: Expressive privacy via obfu-cation *APRJA*, *4*(1), 88-98. https://rednoise.org/daniel/res/pdfs/expressiveprivacy.pdf

Howe, D. y Nissenbaum, H. (2009). *TrackMeNot*. En Kerr, I., Lucock, C. y Steeves, V. (Eds.) *Lessons from the identity trail*. (pp. 417-436). Oxford: Oxford University Press

Lessig, L. (2009). *El Código 2.0*. Traficantes de Sueños.

Nadal, Martín (s.f.) *FANGØ is a defense weapon against surveillance capitalism.* Fango. http://fango.martinnadal.eu/index.html

O'Neill, C. (2017). *Armas de destrucción matemática. Cómo el Big Data aumentala desigualdad y amenaza la democracia*. Capitán Swing.

Pasquale, F. (2015) *The black box society.* Harvard University Press.

Peirano, M. y Snowden, E. (2015). *El pequeño libro rojo del activista en la red.* Roca Editorial. https://acortar.link/HUp0a2

Peirano, M. (2019). *El enemigo conoce el sistema*. Debate. https://acortar.link/Bm0kwH

Perragin, C. y Renouard, G. (2021, julio). Los cables submarinos, un asunto de Estados. *Le Monde Diplomatique en español*. https://mondiplo.com/los-cables-submarinos-un-asunto-de-estados

Pitron, G. (2021, octubre). Cuando la tecnología digital destruye el planeta. *Le Monde Diplomatique en español*. https://mondiplo.com/cuando-la-tecnologia-digital-destruye-el-planeta

Rimbert, P. (2018, febrero). Socialismo digital. *Le Monde Diplomatique en español*. https://mondiplo.com/socialismo-digital

Sabariego, J. (2020, 18 de marzo). Algoritarismos. *El Salto*. https://www.elsaltodiario.com/tecnopolitica/algoritarismos-politica-tecnologia-negocio- algoritmo

Schwartz, P.M. (1989). The computer in German and American constitutional law: Towards an American right of informational self-determination, *The American Journal of Comparative Law Vol. 37*(4), 675-701. https://doi.org/10.2307/840221

Snowden, E. (2019). *Vigilancia permanente.* Planeta.

Submarine Cable Map (s.f.). TeleGeography. Submarine Cable Map. Subnarinecablemap.com. https://www.submarinecablemap.com/

Véliz, C. (2021). *Privacidad es poder. Datos, vigilancia y libertad en la era digital*. Debate.

Zuboff, S. (2020). *La Era del Capitalismo de la Vigilancia*. Paidós.