DEMOCRACIA DE LA VIGILANCIA: DATOS, ACTIVISMO Y CONTRAPODER

SURVEILLANCE DEMOCRACY: DATA, ACTIVISM, AND COUNTER-POWER

Patrici Calvo[1]
Univeristat Jaume I, Castellón de la Plana. España
calvop@uji.es

Carlos Saura García[2]
Universitat Jaume I. Castellón de la Plana. España
saurac@uji.es

Recibido: septiembre de 2024
Aceptado: octubre de 2024

Palabras clave: democracia de la vigilancia; vigilancia social masiva; despotismo democrático; despotismo tecnológico; datactivismo; datahackerismo
Keywords: surveillance democracy; mass social surveillance; democratic despotism; technological despotism; datactivism; datahackerism

Resumen: Esta investigación analiza críticamente el actual contexto sociopolítico y económico de vigilancia masiva para reconstruir las claves y condiciones de posibilidad que orientan su desarrollo en sentido justo y responsable. El estudio, por un lado, advierte del peligro de los impactos disruptivos que produce sobre la sociedad y sus diferentes esferas funcionales la vigilancia social masiva ejercida por los estados y las grandes corporaciones tecnológicas. Por otro, de forma más concreta, sugiere que esta vigilancia social masiva está dando lugar a prácticas despóticas que pervierten los procesos democráticos, reducen los espacios de libertad y aumentan la brecha de las desigualdades. Finalmente, desde sus presupuestos normativos y condiciones de posibilidad, ofrece orientaciones para hacer frente a la vigilancia social masiva: la promoción de una sociedad civil fuerte, dinámica y crítica que actúe como contrapoder frente al estado y las grandes tecnológicas.

1 Esta publicación es parte del proyecto PID2022-139000OB-C22, financiado por MCIU/AEI/10.13039/501100011033/FEDER, UE, así como de las actividades del grupo de investigación de excelencia CIPROM/2021/072 de la Comunitat Valenciana.

2 Esta publicación es parte del proyecto PID2022-139000OB-C22, financiado por MCIU/AEI/10.13039/501100011033/FEDER, UE y ha sido posible gracias a la financiación recibida de la Universitat Jaume I a través de un contrato predoctoral (PREDOC/2022/08).

Abstract: This research critically analyses the current socio-political and economic context of mass surveillance in order to reconstruct the keys and conditions of possibility that guide its development in a fair and responsible sense. The study, on the one hand, warns of the dangers and disruptive impacts underlying the mass social surveillance currently exercised by states and large technological corporations. On the other, it suggests that this mass social surveillance is giving rise to despotic practices that pervert democratic processes, reduce spaces of freedom and increase the inequality gap. Finally, it offers guidelines for confronting mass social surveillance: the promotion of a strong civil society that acts as a counter-power to the state and big tech.

1. Introducción

Durante las dos primeras décadas de siglo XXI, la convergencia sinérgica de varias disciplinas científico-técnicas como el Internet de las Cosas, el Big data, la Robótica, la Inteligencia artificial e incluso la neurotecnología ha dado lugar a la posibilidad de generar, recopilar y explotar datos masivos de todo mediante la recreación y puesta en marcha de ecosistemas ciberfísicos[3]. Este hecho ha propiciado toda una revolución, un momento disruptivo sin precedentes cuyos impactos y consecuencias se están dejando sentir con fuerza en la sociedad y sus diferentes esferas funcionales.

En el ámbito democrático[4], este hecho resulta especialmente significativo. Los datos y metadatos masivos son utilizados por los estados y los mercados para predecir y controlar, incluso manipular en algunos casos, los comportamientos de la ciudadanía y la competencia política o económica con la finalidad de maximizar sus objetivos estratégicos. Los resultados cosechados por aquellos países como China y USA o aquellas organizaciones económicas como Google, Amazon, Meta, Apple y Microsoft (las GAMAM) en occidente y Alibaba, ZTE, Huawei, Baidu, Tencent y Hikvision en oriente, han propiciado toda una lucha global por el poder geopolítico y geoeconómico basado en el control de las tecnologías, los instrumentos y las plataformas que permiten la generación, recopilación y procesamiento de los datos y metadatos masivos disponibles o posibles de la ciudadanía (Helberg,

3 Los ecosistemas ciberfísicos recrean espacios artificiales de información que, estructurados alrededor de programas y dispositivos informáticos, tecnología biométrica e instrumentos de sensorización digitalmente interconectados y virtualmente organizados, controlados y gobernados por algoritmos (algunos dotados de inteligencia artificial), permiten la *hiperconectividad* y *datificación* de toda la realidad física y social, ya sean personas, animales, procesos, elementos o cosas, y los comportamientos asociados (Armenteras et al., 2016; Calvo, 2020).

4 Aquí, se entiende la democracia en un sentido amplio, es decir, no sólo aquellos sistemas políticos cuyos representantes son elegidos por la ciudadanía mediante sufragio, sino también aquellos sistemas de mercado y sociedad civil cuyas organizaciones y empresas implicadas y/o afectadas participan activamente en los procesos de generación de opinión pública.

2021; Hillman, 2021; Webb, 2021; Saura García, 2024).

No obstante, también la sociedad se está posicionado como contrapoder de las políticas y economías de vigilancia a través de movimientos civiles de vigilancia basados en los datos, como el activismo de datos, el ciberactivismo político y los *cyberblowers* (informadores cibernéticos), entre otros. Todo ello ha dado lugar a la irrupción de un nuevo modelo de democracia cuyo principal foco de atención es la vigilancia de sus elementos estructurales a partir de sus datos y metadatos, así como la vigilancia mutua entre las distintas esferas funcionales.

Esta *democracia de la vigilancia*, por consiguiente, hace referencia a la emergencia de un nuevo contexto político, económico y social digitalmente *hiperconectivizado*, *algoritmizado* y *dataficado*. Se trata de una nueva forma de organización del estado, el mercado y la sociedad forjada sobre el *tecno-solucionismo* y la generación, recopilación y explotación de los datos y metadatos que genera la ciudadanía que interactúa a través de los ecosistemas ciberfísicos.

2. Objetivos

Este estudio parte de la hipótesis de que un escenario democrático tan disruptivo como el generado por la transformación digital exige trabajar en la recreación de una sociedad civil fuerte, crítica y dinámica que actúe como contrapoder frente al estado y las grandes tecnológicas. Sólo un estado de equilibrio semejante permitiría la emergencia de democracias maduras capaces de hacer frente a cualquier tipo de despotismo y tiranía tecnopolítica y promover un desarrollo democrático en un sentido justo, responsable y *felicitante*.

Esta hipótesis se basa en un enfoque de democracia de doble vía como el propuesto por Alexis de Tocqueville en el siglo XIX (1990a, b) y desarrollado y ampliado por John Keane (1992),Jürgen Habermas (1998; 2023) o Domingo García-Marzá (2013) entre otros/as en el siglo XX y XXI. A través de este enfoque, Tocqueville y Habermas consiguieron implantar y articular en el núcleo de la teoría democrática el potencial transformador de la realidad social que atesora la sociedad civil, mientras que García-Marzá y Keane entre otros hicieron lo propio mostrando el potencial coercitivo y coordinador de la acción inherente a la sociedad civil e incluyendo a las organizaciones económicas, tanto públicas como privadas, en su entramado asociativo[5].

Apoyándose en esta propuesta de democracia de doble vía, el objetivo principal de este estudio es desvelar y comprender las estructuras y los intereses que subyacen a la democracia de la vigilancia, así como los impactos actuales o virtuales que esta produce sobre la sociedad y la ciudadanía, con el objetivo de proponer orientaciones para su desarrollo práctico. Para ello, en primer lugar, se profundizará en el comportamiento, funcionamiento y objetivos de los gobiernos y mercados de vigilancia más desarrollados basados en

5 Dadas las limitaciones de espacio, no es posible profundizar en la propuesta actual y desarrollada de democracia de doble vía. Para un mayor conocimiento del enfoque, ver Keane (1992), Habermas (1998, 2023) y García-Marzá (2013) entre otros. También es muy aconsejable el concienzudo y esclarecedor estudio realizado por Robinson Dos Santos (2023) sobre la reflexión habermasiana alrededor de la transformación digital de la esfera pública.

los datos y metadatos masivos de la ciudadanía. En segundo lugar, por un lado, se analizará críticamente la expansión de las tecnologías de vigilancia masiva alrededor del mundo y su uso político y económico por parte de organismos gubernamentales y grandes tecnológicas. Y, por otro, se abordarán las características, el funcionamiento y los objetivos de las infraestructuras de vigilancia creadas por las grandes corporaciones tecnológicas y sus impactos sobre la ciudadanía, la opinión pública y los sistemas democráticos. En tercer lugar, se mostrará la emergencia y potencialidad de diferentes movimientos de contrapoder de la sociedad civil frente a los estados y mercados de vigilancia masiva. Finalmente, por un lado, se reflexionará sobre las causas de la asimetría de poder de los sistemas democráticos basados en la vigilancia masiva y sus consecuencias —el empobrecimiento de la capacidad de cambio y transformación de la realidad social de la sociedad civil mediante imperativos sistémicos como el poder y el dinero— y, por otro, se ofrecerán orientaciones para intentar revertir esta tendencia.

3. Metodología

Para conseguir el objetivo, este estudio del ámbito de la filosofía política se ha llevado a cabo en el marco de una propuesta hermenéutico-crítica de análisis, comprensión y prescripción de democracia y sus procesos. Se trata de una metodología propia de las ciencias humanas y sociales que, desde el estudio e interpretación de fuentes bibliográficas y casos prácticos, analiza críticamente el actual contexto sociopolítico y económico de vigilancia masiva para reconstruir los presupuestos normativos que permiten orientar su desarrollo en el marco de una democracia de doble-vía[6], así como las condiciones de posibilidad que permiten su recreación fáctica. Es decir, un enfoque metodológico que se aleja de aquellas posturas cientificistas basadas en la neutralidad y la objetividad para abordar el interés del conocimiento por una mayor emancipación y autonomía del ser humano a través de la comprensión y la crítica.

Para ello, partiendo del problema detectado —el uso de la vigilancia masiva con fines instrumentales, despóticos y tiránicos por parte de corporaciones gubernamentales y grandes tecnológicas— y la hipótesis de partida —la necesidad de promover una sociedad civil de la vigilancia capaz de ejercer como contrapoder del estado y del mercado que utiliza la vigilancia masiva con fines poco democráticos—, en un primer momento se han recopilado y analizado críticamente distintas fuentes bibliográficas especializadas e informes del estado de la cuestión alrededor de la democracia de la vigilancia. Posteriormente, se han recopilado y estudiado casos prácticos sobre la realidad e impactos actuales de la democracia de la vigilancia en la política, la economía y la sociedad civil. Finalmente, mediante la reflexión y comprensión crítica de toda la información generada durante los dos primeros momentos, se ha procedido a la reconstrucción de los presupuestos normativos y condiciones de posibilidad de una democracia de la vigilancia a la altura de lo exigible y deseable por una ciudadanía

6 Por limitaciones de espacio, este estudio no puede abordar en profundidad el método hermenéuticocrítico. Para mayor conocimiento de este método, ver Habermas (1984), Apel (1985), Cortina (1985), Conill (2006, 2008), Cortina et al. (2008) y Nicolas et al. (2023), entre otros.

madura; es decir, con un nivel posconvencional de desarrollo moral.

4. Nacimiento de la vigilancia social masiva

La incapacidad de detectar y predecir las intenciones de los terroristas de los *Atentados del 11S* en 2001 supuso una verdadera consternación para las autoridades de los Estados Unidos. A partir de este momento se produjo un aumento exponencial del interés de estas autoridades por la recopilación, almacenamiento y procesamiento de los datos y metadatos que produce la ciudadanía, así como las naciones y sus diferentes instituciones y organizaciones. El informe realizado por expertos encargado por el gobierno de los Estados Unidos años después sobre los *Atentados del 11S* subraya que en aquel momento,

> Los atentados del 11 de septiembre fueron una demostración gráfica de la necesidad de contar con información detallada sobre las actividades de terroristas potenciales […]. Una parte de esa información, que podría haber resultado de utilidad, no se recopiló, y otra, que podría haber ayudado a impedir los atentados, no fue compartida entre los departamentos[7] (Clarke et al., 2014: 27).

Este informe pone en evidencia que una de las principales causas que impidió pronosticar y anunciar estos atentados fue la falta de intercambio de datos entre los organismos de seguridad de la *Intelligence Community* de los Estados Unidos, entre los que destacan instituciones como el FBI, la CIA y la NSA. A raíz de los sucesos del 11 de septiembre de 2001, el gobierno de los Estados Unidos llegó a la conclusión de que los atentados se hubieran podido evitar si hubiera existido una infraestructura de recopilación, almacenamiento, intercambio y análisis de datos y metadatos dentro de sus organismos de defensa y de seguridad. Por ello, desde el ejecutivo de George W. Bush se promovió la creación de un nuevo escenario mundial donde la recopilación, el intercambio y el análisis de datos y metadatos masivos fuera la base del control de las amenazas de la sociedad estadounidense (Greenwald, 2014; Snowden, 2019). Este nuevo escenario se basó en dos grandes pilares: la creación de una estructura de vigilancia social masiva gestionada por la *Intelligence Community* y la promoción de grandes corporaciones digitales que nutrieran de datos a esta estructura de vigilancia.

Por una parte, se pusieron en marcha un conjunto de herramientas y sistemas de vigilancia social masiva por parte de la *Intelligence Community* de los Estados Unidos y de sus principales países aliados (Australia, Canadá, Nueva Zelanda y Reino Unido), los llamados *Five Eyes*, con seis premisas fundamentales: "Husmea en todo, Entérate de todo, Recógelo todo, Procésalo todo, Aprovéchalo todo, Asócialo todo" (Snowden, 2019). En el centro de este entramado de vigilancia destacan los programas de gestión de datos y metadatos PRISM, Upstream, Trailblazer y XKEYSCORE. En líneas generales estos programas se dedicaban a recopilar y extraer grandes conjuntos de datos de las plataformas e infraestructuras tecnológicas de internet y a combinar, entrelazar y analizar grandes conjuntos de datos y metadatos con el objetivo de vigilar y controlar las actividades de la ciu-

7 Traducción extraída de *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder* (Zuboff, 2020: 737)

dadanía mundial, las empresas nacionales y extranjeras, los estados extranjeros en general y la ciudadanía de los Estados Unidos en particular (Greenwald, 2014; Lyon, 2015; Snowden, 2019).

Por otra parte, la necesidad de disponer de flujos de datos y metadatos de forma constante para poder alimentar a los programas de vigilancia social masiva provocó la necesidad de desregular el contexto de internet y potenciar el crecimiento de corporaciones digitales que estaban empezando a ofrecer multitud de servicios y actividades en el ciberespacio que implicaban a una gran cantidad de usuarios (Snowden, 2019; Zuboff, 2020). Estas corporaciones digitales eran las llamadas GAFAM (Google, Amazon, Facebook, Apple y Microsoft) que con el paso de los años se han convertido en las dominadoras de los grandes conjuntos de datos de las sociedades modernas y en las máximas exponentes del capitalismo de la vigilancia y de su modelo de negocio. Esta situación fue aprovechada por las GAFAM para generar unos grandes beneficios económicos a partir de un nuevo modelo de negocio basado en los datos y metadatos e introducirse y consolidarse entre las principales corporaciones del planeta, y por la *Intelligence Community* estadounidense para obtener acceso a los datos y metadatos de estas corporaciones ya sea a través de resoluciones judiciales, acuerdos entre las corporaciones y el gobiernos ocultos a la opinión pública o por medio de acciones clandestinas (Greenwald, 2014; Snowden, 2019).

El nuevo escenario de explotación de datos y metadatos por parte de los gobiernos y del mercado posterior a los *Atentados del 11S* provocó multitud de interdependencias entre estos grupos y fue el pistoletazo de salida de la utilización política y económica de los grandes conjuntos de datos y metadatos, que ha ido evolucionando y perfeccionándose hasta nuestros días. Por un lado, el desarrollo de los ya citados programas de vigilancia social masiva permitió a la *Intelligence Community* rastrear y analizar todos los comportamientos, acciones o actividades presentes o pasadas de cualquier persona que utilizase cualquier dispositivo digital enmarcado dentro de un ecosistema ciberfísico a partir de los datos y metadatos de las grandes corporaciones digitales. Por otro lado, el crecimiento de las GAFAM dio lugar a un capitalismo de la vigilancia que ha colocado a los datos y metadatos como materia prima de las principales compañías del planeta y ha provocado una mercantilización de los datos privados de los ciudadanos con el objetivo de conseguir beneficios económicos. Snowden profundiza en la gravedad que supone esta situación,

> No podemos permitir que la «vigilancia de Dios» a la que estamos sometidos se use para «calcular» nuestros puntos de ciudadanía o para «predecir» nuestra actividad criminal; para decirnos qué clase de educación podemos recibir, o qué tipo de trabajo podemos tener, o si podemos recibir educación o tener un trabajo, directamente; para discriminarnos por nuestros historiales económicos, legales y médicos, por no mencionar nuestra etnia o raza, constructos que a menudo los datos asumen o imponen. Y con respecto a nuestros datos más íntimos, es decir, a nuestra información genética, si permitimos que la utilicen para identificarnos, entonces la utilizarán para acosarnos, e incluso para modificarnos: para rehacer la esencia misma de nuestra humanidad a imagen de la tecnología que pretende hacerse con su control. Por supuesto, todo eso ya ha pasado (Snowden, 2019: 437-438).

Este fragmento subraya que el contexto de vigilancia social masiva permanente originó una situación, prolongada hasta la actualidad, en la que los centros de poder tanto políticos como económicos conocen y explotan prácticamente la totalidad de los datos y metadatos de la ciudadanía con el objetivo de controlar a cada ciudadano e influenciar y manipular su com-portamiento, su ideología y su opinión. A pesar de que la infraestructura de vigilan-cia ilegal, clandestina y oculta de la *Intelli-gence Community* de los Estados Unidos fue descubierta y parcialmente desman-telada a partir del 2013 (Gellman et al., 2013; Greenwald et al., 2013; Macaskill y Dance, 2013; Emmerson, 2015), las GA-FAM (ahora GAMAM, debido al cambio de nombre de Facebook por Meta) y otras grandes corporaciones digitales orientales han desarrollado nuevas y potentes infraestructuras de vigilancia y control que utilizan para influenciar y manipular a la ciudadanía que afectan directamente a la democracia y a su correcto funcionamiento.

5. Política y economía en un contexto de vigilancia social masiva

El informe realizado en 2019 por Steven Feldstein titulado *The Global Expansion of AI Surveillance* analiza la utilización y la expansión de las tecnologías de vigilancia disruptivas vinculadas con el *big data* y la Inteligencia Artificial en el mundo durante la última década (Feldstein, 2019). Este informe destaca especialmente tres as-pectos.

El primero de ellos, es que se ha produ-cido un gran crecimiento de la utilización de infraestructuras de vigilancia social por parte de una gran cantidad de gobiernos de países. Al menos 75 de los 176 países del mundo utilizan activamente este tipo de infraestructuras para propósitos como son la vigilancia, monitorización y control indiscriminado de la ciudadanía, las restricciones y desconexiones de internet en determinadas zonas y periodos, la personalización de contenidos, la difusión de desinformación o la manipulación de procesos electorales. El segundo y más sorprendente es que las democracias avanzadas son las mayores usuarias de las tecnologías de vigilancia social masiva[8]. El tercero de ellos es que China y sus grandes corporaciones digitales se han convertido en importantes suministradoras de tecnologías en todo el mundo, especialmente en el campo de las tecnologías de vigilancia social masiva. Durante los últimos años el gobierno chino ha copiado el modelo de los Estados Unidos y ha potenciado a un conjunto de corporaciones digitales, entre las que destacan Alibaba, ZTE, Huawei, Baidu, Tencent y Hikvision, las cuales monopolizan y dominan el contexto digital en China y se han introducido en multitud de países alrededor del mundo (Webb, 2021).

Los tres aspectos que subraya este informe describen una situación global en la cual las infraestructuras y las tecnologías relacionadas con la vigilancia social masiva se están desarrollando y extendiendo a una gran velocidad por multitud de estados que van desde las democracias avanzadas hasta los estados autocráticos. Detrás de esta situación que se podría

8 El 51% de las democracias avanzadas, el 41% de los estados autocráticos competitivos, el 41% de las democracias iliberales y el 37% de los estados autocráticos cerrados implementa sistemas de vigilancia social masiva (Feldstein, 2019).

describir como de vigilancia global masiva, se esconde una cruenta guerra geopolítica y geoeconómica entre las corporaciones tecnológicas de los Estados Unidos y las corporaciones tecnológicas de China por el suministro de tecnologías disruptivas basadas en la explotación de grandes conjuntos de datos y metadatos y por la colonización y dominación de estos conjuntos de datos y metadatos a nivel global (Saura García, 2024).

La batalla entre los dos grupos de corporaciones digitales se juega en diversos campos como son las aplicaciones, las infraestructuras de software, los sistemas de hardware o la infraestructura de transporte de datos y metadatos (cables submarinos, redes de fibra óptica, redes de telefonía y de internet o estaciones de 5G) (Hoffman y Attrill, 2021) y en la aplicación y expansión de todo este conjunto tecnológico a través de planes y proyectos tanto gubernamentales como comerciales que permitan a estas corporaciones dominar grandes conjuntos de datos y metadatos con el objetivo de lograr propósitos estratégicos tanto políticos como económicos (Cave et al., 2019; Ryan et al., 2019).

Las grandes corporaciones digitales de los Estados Unidos, pioneras de la utilización de tecnologías de explotación de grandes conjuntos de datos y metadatos, han logrado una fuerte penetración en la economía mundial como consecuencia de la amplia gama de servicios, plataformas e infraestructuras de software, de hardware y de transmisión de datos y metadatos de las GAMAM utilizados diariamente por miles de millones de personas y en la política gracias al desarrollo de proyectos militares o de vigilancia social masiva en colaboración con múltiples gobiernos (Feldstein, 2019; Snowden, 2019; Zuboff, 2020).

La dominación y utilización conjunta de grandes paquetes de datos y metadatos vinculados con la comunicación, la economía y la política han permitido a las GAMAM crear una potente infraestructura de producir beneficios económicos basada en la monetización de datos y en la vigilancia de la ciudadanía denominada capitalismo de la vigilancia (Bartlett, 2018; Moore, 2018; Zuboff, 2020; Han, 2021). El actual modelo de negocio de las GAMAM hace posible el control y modificación de la conducta y la ideología de la ciudadanía en beneficio propio a partir de métodos disruptivos que eluden la decisión humana, la autonomía o la autodeterminación personal incidiendo de forma decisiva en la opinión pública y los procesos democráticos (Zuboff, 2020; Han, 2021). Durante la última década se han podido confirmar multitud de operaciones de influencia, manipulación y modificación de opinión pública y de procesos democráticos, que han implicado en mayor o menor medida a las GAMAM, como por ejemplo los casos de Polonia, Alemania, Brasil, Canadá, Taiwán, Ucrania, Reino Unido o Estados Unidos (Woolley y Howard, 2018; Howard, 2020; Woolley, 2023).

Las grandes corporaciones tecnológicas de China, escoltadas y potenciadas en todo momento por el gobierno y el Partido Comunista de China[9], se han desarrolla-

9 El sector de las grandes corporaciones tecnologías dispone de múltiples acuerdos de colaboración en diversas materias con el gobierno chino y es el que contiene la mayor proporción de dirigentes del Partido Comunista Chino en sus puesto directivos de todos los sectores económicos del país (Cave et al., 2019; Hoffman y Attrill, 2021).

do ampliamente dentro y fuera de China desde la llegada al poder de Xi Jinping (Hannig, 2019; González, 2021). En un primer momento, las tecnologías y los grandes conjuntos de datos y metadatos de estas corporaciones fueron utilizadas por el gobierno chino para constituir la infraestructura de vigilancia social masiva más desarrollada del planeta hasta el momento dentro de sus fronteras. Las principales herramientas de control, vigilancia y represión de esta infraestructura son el sistema de crédito social digital, el cual otorga una puntuación a cada uno de los ciudadanos chinos en relación a sus comportamientos, los sistemas de vigilancia orwelliana desarrollados en grandes ciudades y vías de comunicación y el programa denominada *The Great Firewall* dedicado a la censura, control y vigilancia de contenidos, opiniones y comportamientos de la ciudadanía en la red (Jiang y Fu, 2018; Hannig, 2019; Lee, 2020).

Una vez logrado esto, China ha potenciado el crecimiento internacional de sus corporaciones a través de la llamada *Belt and Road Initiative* (BRI) (Kliman et al., 2019; Helberg, 2021; Hillman, 2021). Esta iniciativa hace referencia a la creación de una amplia red de infraestructuras físicas y digitales en el resto del mundo que abarca desde la difusión de plataformas sociales y el desarrollo de infraestructuras comerciales y de telecomunicaciones hasta la puesta en marcha de proyectos de vigilancia social masiva encargados por otros estados[10] (Feldstein, 2019; Kliman et al., 2019). La punta de lanza del BRI es la difusión del modelo digital chino más allá de sus fronteras con la intención de exportar su modelo de autoritarismo digital. El avance del autoritarismo digital a través de las grandes corporaciones tecnológicas chinas «is being promoted as a way for governments to control their citizens through technology, inverting the concept of the internet as an engine of human liberation» (Shahbaz, 2018). La expansión de la tecnología china aparentemente es beneficiosa política y económicamente tanto para los gobiernos como para la ciudadanía proveída de sus infraestructuras, pero suscita importantes preocupaciones relacionadas con la pérdida de soberanía de los gobiernos y de la ciudadanía, la imposición de las normas morales y éticas chinas y la manipulación de los procesos democráticos en favor de los objetivos políticos y económicos del gobierno chino (Feldstein, 2019; Helberg, 2021; Hillman, 2021)

El avance del modelo digital chino en realidad supone la pérdida del control de las operaciones, las gestiones, las infraestructuras digitales y los grandes conjuntos de datos y metadatos producidos por los ecosistemas ciberfísicos y la ciudadanía por parte de los gobiernos nacionales y de otras grandes corporaciones tecnológicas a nivel mundial, mayormente estadounidenses, para ser asumido directamente por las grandes corporaciones chinas e indirectamente por el Partido Comunista de China (Cave et al., 2019; Kliman et al., 2019; Helberg, 2021).

10 Dentro de la BRI destacan proyectos como el desarrollo de *Smart City-Public Security projects* en ciudades alemanas y francesas como son Gelsenkirchen, Duisburgo, Valenciennes o Marsella, programas de vigilancia y control de la ciudadanía en Venezuela, Zimbabue o Bielorrusia, el desarrollo de una zona económica portuaria especial en Myanmar, la concesión de la gestión del puerto de Atenas en Grecia, la construcción de líneas de alta velocidad en países como Rumania, Serbia y Hungría o la difusión mundial de la plataforma social Tik Tok (Cave et al., 2019; Kliman et al., 2019).

Las grandes corporaciones estadounidenses y las grandes corporaciones chinas están dirigidas hacia propósitos muy diferentes. Mientras las corporaciones americanas se centran en obtener a toda costa beneficios económicos, las corporaciones chinas tienen como objetivo difundir y potenciar el autoritarismo digital (Zuboff, 2020; Webb, 2021). Ambos formatos implican grandes asimetrías de conocimiento y poder entre las corporaciones y la ciudadanía y suponen un verdadero peligro para el correcto funcionamiento de las democracias.

En el formato de las corporaciones estadounidenses se promociona un capitalismo de la vigilancia que pone a disposición de los intereses de los mercados sus grandes conjuntos de datos y metadatos y sus tecnologías disruptivas (Zuboff, 2020). Esta situación pone al abasto de cualquier actor la posibilidad de adquirir grandes conjuntos de información de la ciudadanía e influenciar y manipular sus comportamientos, su ideología o sus opiniones de forma interesada. Hay que destacar que después del escándalo de espionaje de la *Intelligence Community* de los Estados Unidos destapado por Snowden en 2013 el gobierno estadounidense tiene más dificultades para acceder y utilizar los conjuntos de datos de estas corporaciones (Snowden, 2019). En cambio, las grandes corporaciones digitales chinas son utilizadas como infraestructuras de promoción del autoritarismo digital promulgado por el Partido Comunista Chino basado en la exportación de sus normas morales y éticas, en la erosión de la soberanía de los países y en socavar las democracias por medio de la vigilancia ubicua de la ciudadanía y la explotación de grandes conjuntos de datos y metadatos (Cave et al., 2019; Ryan et al., 2019; Webb, 2021).

6. Hacia una democracia de la vigilancia: estado, mercado y sociedad civil

La vigilancia, *per se*, no tiene por qué ser una práctica maliciosa. De hecho, tal y como sugirió Tocqueville en sus trabajos (1990a, b), el escrutinio mutuo y continuado entre las diferentes esferas implicadas en y afectadas por las democracias modernas (estado, mercado y sociedad civil), es condición de posibilidad de su buena salud y desarrollo. Por un lado, el escrutinio mutuo promueve el ejercicio de la libertad, principal antídoto frente a la tiranía de las mayorías y el despotismo democrático. Por otro, el escrutinio mutuo fomenta estados óptimos de equilibrio entre libertad e igualdad, pero también fraternidad (hoy solidaridad), condición necesaria contra la deriva democrática que provoca la priorización o el olvido de cualquiera de estos tres principios[11]. No obstante, el principal problema del contexto actual de la democracia de la vigilancia es la tiranía algorítmica y el des-potismo de los datos que el estado y el mercado ejercen sobre la sociedad civil. Dicho de otro modo, los imperativos

11 Para Tocqueville, cuando las democracias priorizan la libertad frente a la igualdad, producen sistemas anárquicos con niveles de caos, desorden e incertidumbre tan inasumibles que impiden su gobernabilidad. Cuando las democracias priorizan la igualdad frente a la libertad, generan sistemas mudos y despóticos con niveles de tiranía, despotismo y anacronismo tan inasumibles que producen pérdida de sentido y déficits de credibilidad entre la ciudadanía. Cuando las democracias dan la espalda a la fraternidad (solidaridad), generan sistemas paternalistas con niveles de individualismo tan inasumibles que producen desafección y lastran el progreso (Tocqueville, 1990a).

sistémicos que, como el poder y el dinero, tra-dicionalmente han hecho servir el estado y el mercado para colonizar el *mundo de la vida* —mundo objetivo, intersubjetivo y subjetivo— (Habermas, 1987), hoy son complementados —incluso superados— por el monopolio de los datos y metadatos masivos tanto públicos como privados e íntimos de la ciudadanía digitalmente hiperconectada y sus herramientas digitales de *dataficación*, extracción y explotación.

En las últimas décadas, la sociedad civil también ha utilizado los ecosistemas ciberfísicos y los datos y metadatos masivos que produce para ejercer el contrapoder sobre la esfera gubernamental y econó-mica, examinando, controlando y visibi-lizando sus movimientos, actividades e impactos. Destacan al respecto algunos movimientos de vigilancia y contrapoder corporativo y gubernamental que utilizan los datos y metadatos (van Dijck, 2014), como el activismo de datos, el activismo digital[12], el *whistleblowing*, el *hackerismo* ético, el *cyberpunk* o el *cypherpunk*, por citar algunos de los más influyentes.

12 Como afirma Mary Joyce, "The context of digital activism refers both to the digital technology that is used in a given activism campaign and to the economic, social, and political context in which such technology use occurs. Digital technology infrastructure—the combination of networks, code, applications, and devices that make up the physical infrastructure of digital activism—is a starting point but not an ending point. Differences in economic, social, and political factors ultimately alter how activists use this technology. (…) The media have recently been abuzz with cases of citizens around the world using digital technologies to push for social and political change—from the use of Twitter to amplify protests in Iran and Moldova to the thousands of American nonprofits creating Facebook accounts in the hopes of luring supporters" (Joyce, 2010, p. 2).

Datactivismo

El *activismo de datos* es un movimiento ciudadano de carácter científico-técnico y social que ha cogido fuerza en la última década por diferentes motivos e intereses, pero todos ellos complementarios y alineados. Por un lado, como forma de promover el cambio social a través de los medios de comunicación (Sampedro, 2014; Liboiron, 2014, 2015; Gutiérrez, 2018; Milan y Gutiérrez, 2020). Por otro lado, como respuesta frente a las nuevas técnicas de control basadas en algoritmos inteligentes que están haciendo tambalear los cimientos de la democracia y las bases de la ciudadanía (Caffarena, 2017; Sastre y Gordo, 2019). Finalmente, como contrapoder frente a la vigilancia masiva que los gobiernos y las corporaciones ejercen sobre la sociedad civil a través de los ecosistemas ciberfísicos y los fenómenos que le subyacen: *hiperconectividad, dataficación* y *algoritmización* (van Dijck, 2014; Morozov, 2018; Calvo 2020; García-Marzá y Calvo, 2024). Como argumenta Max Liboiron,

> If activism is about changing the relations, assumptions, and contests pertaining to power, then data activism is about using data as a central tactic to make these changes. "Data activism" is not a term of art academia, but it is used in activism, where it usually refers to persuasively leveraging data to launch action (Liboiron, 2014).

Para ello, centrándose especialmente en el último de sus intereses, el *(ciber)activismo de datos* se apropia de la misma infraestructura de vigilancia masiva que utilizan los gobiernos y las corporaciones —como las TIC, los ecosistemas ciberfísicos, las redes sociales, las nubes y las grandes bases de datos, las tecnologías de procesamiento y análisis de datos ma-

sivos, los algoritmos de IA, etcétera— con el objetivo de desvelar y denunciar la tiranía y el despotismo de los datos y otros casos de mala praxis económica y política, concienciar sobre los peligros de la vigilancia masiva y la *datificación* de las relaciones sociales, generar opinión pública y sembrar sentimientos *pro-* y *re-* activos entre la ciudadanía que estimulen su activismo político y corporativo, promuevan su empoderamiento digital y fomenten su compromiso e implicación en los procesos de transformación social.

> If activism is the activation of groups of individuals to achieve a collective aim, then activism in a fundamental sense relies on engaging the underlying forces of community and culture at work in a particular media or space. An activist trying to get the word out about a particular issue in traditional media, for example, will be best equipped when armed with the knowledge of how communities and cultures form around television broadcasts and how best to present information within that medium (Hwang, 2010: 122).

De esta forma, el *(ciber)activismo de datos* se convierte en una actividad de contrapoder democrático que promueve estados óptimos de equilibrio entre libertad, igualdad y solidaridad a través de la crítica, la participación, la afectividad, el asociacionismo, el acuerdo intersubjetivo y el cambio social.

Al respecto, destaca el caso francés durante el último lustro. En este país europeo, el primero en legislar la vigilancia masiva (Labonde, Malhuret, Piedallu y Simon, 2021; La Quadrature du Net, 2023), la ciudadanía de varios núcleos urbanos importantes como Valenciennes, Marsella, Niza, Montpelier o París, pero también de algunas pequeñas localidades como Vallon de Aveyron, se han movilizado e incluso revelado contra el programa *Big Data Public Tranquility* financiado con dinero de la Unión Europea y aplicado gracias a corporaciones tecnologías chinas como Huawai y ZTE y francesas como Engie Ineo y SNEF. Estas herramientas, similares a la controvertida PredPol que utilizan ciudades como Los Ángeles: "(...) analiza los datos proporcionados por la policía, las estaciones de bomberos y los hospitales de la ciudad para anticipar dónde y cuándo podría ocurrir un crimen futuro" (Meaker, 2022), pero también, como en el caso de Niza, detectar y codificar emociones entre los viajeros de los medios de transportes (Violaine, 2019).

> Es el tecno-solucionismo. Existe un problema político y prometen encontrar una tecnología, una app, para controlarlo (...). Es muy costoso y utiliza una parte del dinero de los contribuyentes para implementar soluciones que son peligrosas para las libertades, aumentan el control y son en parte ineficaces (Macdonald, 2022).

Como contrapartida, han surgido movimientos activistas como *Technopolice*, dedicado a mapear y difundir en su plataforma digital la ubicación de las cámaras de vigilancia de las ciudades francesas, y *La Quadrature du Net*, preocupado por defender los derechos digitales de la ciudadanía y detener el uso de la videovigilancia en Marsella. La presión de estos y otros grupos ha sido tal, que ha logrado concienciar y movilizar grandes grupos de ciudadanos y ciudadanas para su causa y llamar la atención de la prensa mundial (Labonde, Malhuret, Piedallu y Simon, 2021).

Datahackerismo

Tradicionalmente, el *hackerismo* es un término que suele vincularse con un agre-

gado de acciones autointeresadas, ilegales y maliciosas, especialmente aquellas que atacan las vulnerabilidades de los sistemas informáticos de organizaciones gubernamentales, económicas y financieras, pero también de la ciudadanía expuesta, para conseguir algún tipo de recompensa personal en clave de beneficio o utilidad. No obstante, el *hackerismo* no puede vincularse sólo ni mayoritariamente con comportamiento dañinos para la sociedad y sus diferentes esferas funcionales[13]. Como describió y definió Kenneth Einar Himma en *Internet security: hacking, counterhacking, and Society* (2007), los móviles de la acción del *hacker* también pueden estar vinculados con algún tipo de resultado positivo para los estados, las economías y, sobre todo, las sociedades. Por ejemplo, con una mejora de los sistemas de seguridad de las instituciones y organizaciones pública y privadas; con la alfabetización digital de la ciudadanía y con una visibilización y/o corrección de aquellos abusos que, como la vigilancia masiva con fines despóticos, cometen algunos gobiernos y organizaciones corporativas sobre la sociedad, produciendo vulnerabilidades y debilitando su progreso (Semenzin, 2017).

En este caso, el *hackerismo* se aleja del *free-rider informático*, aquellas personas que se aprovecha en su propio beneficio de las vulnerabilidades de los sistemas de seguridad de las organizaciones económicas y gubernamentales, y se asemeja a una especie de *centinela* o *protector informático* de la sociedad que actúa en la sombra. En este caso, a la acción se la denomina *hacktivismo ético* y a las personas implicadas se les llama *hackers éticos.*

Entre los muchos casos de *hacktismo ético*, destacan iniciativas como *Cryptoparty* (Semenzin, 2017) por su vinculación con la vigilancia masiva. *Cryptoparty*, que se define a sí mismo como "(...) un movimiento descentralizado con eventos alrededor de todo el mundo" que pretende llevar conocimiento e información a la sociedad acerca de cómo proteger su espacio digital y sus datos (Cryptoparty, 2024), surge en 2012 fuertemente motivada por el shock que produjo en la sociedad la filtración sobre la vigilancia masiva perpetrada durante años por la NSA estadounidense y como respuesta al proyecto de ley *Cybercrime Legislation Amendment Bill* del gobierno australiano (Semenzin, 2017). El principal objetivo de la red consiste en "(...) introducir en la sociedad las herramientas básicas necesarias para la protección de la privacidad, el anonimato y la seguridad en Internet" (Semenzin, 2017). Para ello, ofrece información y orientación a la ciudadanía sobre cómo incluir comunicaciones encriptadas, evitar el seguimiento y vigilancia durante las búsquedas web, e integrar mecanismos de seguridad en los ordenadores personales y terminales móviles (Cryptoparty, 2024).

Datawhistleblowing

En todo ello ha jugado un papel muy importante el *activismo whistleblowing*[14], un movimiento vinculado con aquel "(…)

13 Esta dualidad ha generado un concepto alternativo, el del *crackerismo*, para definir a los hackers maliciosos o autointeresados.

14 El neologismo *whistleblowing* fue acuñado por Ralph Nader durante la *Conference on professional responsibility* celebrada en Washington D.C. el 30 de enero de 1971 (Boffey, 1971: 549-551).

acto de un hombre o una mujer que, creyendo que el interés público prevalece sobre el interés de la organización a la que sirve, públicamente «hace sonar el silbato» si la organización está involucrada en actividades corruptas, ilegales, fraudulentas o perjudiciales" (Nade, Petkas y Blackwell, 1972, VII). Las personas vinculadas con el movimiento se conocen como *whistleblowers*, y se definen como todo aquel ciudadano crítico que, comprometido con los principios y valores de la organización en la que trabaja y de la sociedad en la que vive, es capaz de alertar y/o denunciar públicamente las irregularidades ético-legales que se cometen en el ejercicio de una actividad concreta aun cuando son conscientes del alto coste que puede llegar a pagar por ello, como la pérdida del puesto de trabajo, el fin de una prometedora carrera, el desprecio y descrédito del sector y sus profesionales, el exilio, el ostracismo, la cárcel o, incluso, la muerte (Calvo, 2016). Ernest Fitzgerald y el fraude en las Fuerzas aéreas de EE.UU., Frank Serpico y la corrupción policial en la ciudad de New York, Daniel Elsbergs y los Papeles del Pentágono; Peter Buxton y la protección de los sujetos de investigación en el experimento Tuskegee, William Mark Felt y el caso Watergate, Philip Agge y las malas prácticas de la CIA, Karen Silkwood y las irregularidades en salud y seguridad de Kerr-McGee, Mordechai Vanunu y el programa nuclear israelí, Jeffrey Wigand y los problemas de salud pública de la industria del tabaco; Juan Walterspiel y los ensayos clínicos de la farmacéutica Pfizer, Sherron Watkins y las prácticas contables de la energética Enron; Cynthia Cooper y las prácticas contables de Worldcom; Bradley Manning y los documentos clasificados publicados en WikiLeaks; Edward Snownen y el espionaje masivo de la NSA; Coolen Rowley y las fallas e inacción del FBI en la prevención de los Atentados del 11S; Kostas Vaxevanis y la lista Lagarde, Eric Ben-Artzi y la contabilidad fraudulenta del Deutsche Bank, Jaime González y el cártel del fuego, Brittany Nicole Kaiser y Christopher Wylie y el escándalo de Cambridge Analytica[15] (Nader, Petkas y Blackwell, 1972; Vandekerckhove, 2006; Calvo, 2016, Calvo y Osal, 2018; Vaughn, 2020; Mueller, 2020; Saura García, 2023), son algunos de los casos que mayor impacto han tenido en la sociedad y sus distintas esferas funcionales[16], pero no los únicos[17].

En general, la cultura *whistleblowing* y el interés de los *whistleblowers* no tiene por qué encajar con los parámetros actuales del llamado *activismo de datos* y el *hackerismo ético*. Éste se centra en informar sobre todo tipo de irregularidades y malas prácticas institucionales y corporativas, y su actividad emergió en la década de los 70 (Calvo, 2016; Calvo y Osal, 2018), va-

15 A diferencia de antaño, cuya actividad externa estaba basada casi exclusivamente en los medios de comunicación de masas tradicionales, especialmente los periodísticos y, en menor medida, la televisión, en la actualidad el *whistleblowing* se encuentra estrechamente ligado con el ciberespacio y la esfera pública digital. Al respecto, véanse casos de *whistleblowing* desde 2010.

16 En algunas ocasiones, como el caso de Jack Teixeira y su filtración de documentos del Pentágono sobre la guerra de Ucrania entre 2022 y 2023, se confunde el *narcisismo de datos* con el *activismo de los whistleblowers*. El caso de Jack Teixeira nada tiene que ver con el *whistleblowing*.

17 En muchos casos *whistleblowing*, la identidad de los *whlistleblowers* continúa siendo desconocida, como los que destaparon los sonados escándalos *Luxleaks*, *Panamá papers* y *Paradise papers* entre otros.

rias décadas antes de los fenómenos de la vigilancia masiva y la algoritmización de las esferas funcionales de la sociedad. No obstante, actualmente su actividad está intrínsecamente relacionada con el *(ciber)activismo de datos* (Gutiérrez-Rubí, 2014), puesto que ofrece pistas, datos o información relevante al *(ciber)activismo de datos* para poder desarrollar su actividad en sus diferentes facetas: denuncia, concienciación, transformación social, contrapoder, empoderamiento, etcétera.

Activismo de datos, *hackerismo* ético y *whistleblowing* son algunos ejemplos de la capacidad de la sociedad civil para postularse como contrapoder en la era de la vigilancia masiva. No obstante, durante la última década las grandes corporaciones gubernamentales y corporaciones tecnológicas han aumentado su despotismo sobre la sociedad civil para garantizar la asimetría de poder y el control efectivo de la sociedad de la vigilancia a través, como diría Habermas (1987), de imperativos sistémicos como el poder y el dinero, pero hoy también los datos masivos y las tecnologías inteligentes.

7. Del despotismo democrático al ludismo de datos

Para Tocqueville, la clave de una buena democracia se halla en el correcto equilibrio entre sus principales esferas —el estado, el mercado y la sociedad civil— y valores —libertad y igualdad—. Los desequilibrios funcionales y axiológicos producen altos niveles de desincronización y entropía social en las democracias modernas, generando su deriva hacia sistemas despóticos basados en la tiranía de las mayorías, el estatismo intelectual, el individualismo social, el paternalismo institucional y la servidumbre legislativa (Tocqueville, 1990a, b). Este despotismo democrático, como afirma Tocqueville, genera la bajeza y vulgaridad moral de las instituciones democráticas y la degeneración de las costumbres públicas y los procesos democráticos (Tocqueville, 1990b).

En la última década, tanto los organismos gubernamentales como las grandes corporaciones tecnológicas han puesto en marcha prácticas despóticas de captación y contratación de *datactivistas*, *hackeréticos (ethical hackers)* y *cyberwhistleblowers*, así como con otros grupos implicados en el activismo político y corporativo, basadas en suculentos beneficios económicos, fiscales y/o legales para que colaboren con ellos y para ellos.

En la esfera estatal, destaca el *Launches Pilot Project Challenging* Hackers *to Test Federal Cyber Security* y otras llamadas para la contratación de hackers *(Call for hackers)* llevadas a cabo por el Pentágono y otros organismos gubernamentales de los EE.UU. en la última década para mejorar su ciberseguridad y minimizar sus cibervulnerabilidades (CNN, 2012; Moser, 2016; Jiménez, 2016; Syeed, 2017). Como desveló Nafeesa Syeed, "The Pentagon is paying hackers to test its key internal systems for vulnerabilities—and they are finding weaknesses faster than expected" (Syeed, 2017).

En la esfera mercantil, destacan los casos de contratación, reconocimiento público e incentivación de hackers éticos por parte de grandes tecnológicas como Apple, Google, Amazon, etcétera (La Información, 2011; AppleInsider Staff, 2016). Por ejemplo, los *Pwnie Award* (2007-2022) a las mejores prácticas *hacker* en el ám-

bito de la ciberseguridad (Pwnie Award, 2023), el reto Google retribuido con 2,7 millones de dólares como máximo a quien consiguiera *hackear* el sistema Chrome OS (2013-2016).

Estas prácticas despóticas vacían la esfera de la sociedad civil de sus entidades y elementos digitalmente más empoderados, limitando su libertad y debilitando su capacidad de acción y contrapoder frente a las prácticas de vigilancia de esferas como el estado y el mercado. De ahí la emergencia de movimientos neoluditas —como el ludismo 4.0, el dataludismo o el Camover— contra el despotismo de los datos.

Indicios de este renacer del movimiento ludita se han podido observar y sentir en las protestas hongkonesas de 2019 contra el despotismo y la opresión del gobierno chino, cuando un grupo de manifestantes tumbó una torre con cámaras de reconocimiento facial instalada por el gobierno chino para vigilar a la ciudadanía, así como en la retirada del robot Digidog que utilizaba el Departamento de Policía de Nueva York para patrullar las calles ante las reacciones muy negativas que empezaba a suscitar entre la ciudadanía. Pero, sobre todo, destaca el movimiento Camover surgido de las calles de Berlín y exportado a otros lugares y países[18] cuyo objetivo es destruir o inutilizar cámaras de vigilancia masiva. Como explica Oliver Stallwood en *The Guardian*,

> The rules of Camover are simple: mobilise a crew and think of a name that starts with "command", "brigade" or "cell", followed by the moniker of a historical figure (Van der Lubbe, a Dutch bricklayer convicted of setting fire to the Reichstag in 1933, is one name being used). Then destroy as many CCTV cameras as you can. Concealing your identity, while not essential, is recommended. Finally, video your trail of destruction and post it on the game's website — although even keeping track of the homepage can be a challenge in itself, as it is continually being shut down (Stallwood, 2013)

Evitar que estas prácticas *dataludistas* suban en número e intensidad y se conviertan en un lastre para la buena salud de las democracias modernas, exige la erradicación del despotismo democrático y corporativo imperante, así como del *dataempoderamiento* de la sociedad civil. Porque, como argumentaba Tocqueville (1990b), una de las misiones más importantes de un sistema democrático radica en enseñar a la ciudadanía a prescindir del sistema político, a sentir y ejercer la libertad, a participar de lo público, a no ser dependientes del estado para encontrar solución a los problemas y proyectarse una vida buena.

> Se diría que los soberanos de nuestra época sólo intentan hacer grandes cosas con los hombres. Quisiera que pensasen un poco más en hacer grandes hombres, que concedieran menos valor a la obra y más al obrero, que recordasen constantemente que una nación no puede permanecer fuerte mucho tiempo cuando cada hombre es individualmente débil y que no se han encontrado formas sociales y combinaciones políticas que puedan hacer enérgico a un pueblo compuesto de ciudadanos pusilánimes y lánguidos (Tocqueville, 1990b: 386).

Para ello, cabe dejar de coartar la libertad de acción, participación y cooperación de y entre los diferentes grupos implicados en el activismo político y corporativo, promover su activismo como un bien democrático que merece ser potenciado

18 En otros países, como España, y ciudades, como Badajoz, ya se han registrado casos similares (Reigadas, 2022).

y preservado y empoderar a los/as activistas a través del acceso y la mejora a los recursos y los datos (*open resources* y *open data*) que permiten la vigilancia como contrapoder de la sociedad civil y, con ello, el equilibrio óptimo mutuamente beneficioso entre las tres esferas de la democracia.

8. Conclusiones

Como se ha intentado mostrar en este estudio, las democracias se centran cada vez más en el control, explotación y uso de los datos y metadatos masivos que produce la ciudadanía digitalmente hiperconectada. Disponer de un acceso ilimitado a los datos y metadatos y de una tecnología inteligente capaz de recopilarlos, almacenarlos y procesarlos para convertirlos en información relevante primero y conocimiento aplicable después, es visto por los gobiernos estatales como el principal instrumento de mejora y desarrollo político, económico y social. No obstante, el fenómeno de la vigilancia masiva se ha convertido en un arma de doble filo para las democracias.

Por un lado, los gobiernos y las grandes corporaciones tecnológicas justifican la puesta en marcha de técnicas y tecnología de vigilancia masiva por los grandes beneficios extrínsecos que produce para la sociedad, como un aumento y mejora de la salud y seguridad de la sociedad; de la capacidad de captación y comprensión de la opinión pública; de la posibilidad de elaborar leyes y políticas públicas más objetivas, eficientes y cercanas a las expectativas y necesidades de la ciudadanía; de establecer procesos democráticos más inclusivos, participativos y robustos, y del diseño de mercados más competitivos, responsables y sostenibles.

Por otro, se observa que el uso actual de la vigilancia masiva por parte de los gobiernos y las grandes corporaciones tecnológicas ha derivado o está derivando hacia prácticas despóticas que pervierten los procesos democráticos y aumentan la tiranía de los grandes centros de poder, la instrumentalización de la ciudadanía y la bajeza e inopia moral de las instituciones y organizaciones democráticas. Destacan al respecto aspectos como el uso fraudulento e indiscriminado de tecnología de reconocimiento facial, la manipulación de la opinión pública mediante la producción masiva de datos sintéticos en la esfera pública, la reducción de los espacios de libertad y participación ciudadana, o la generación de oligopolios de datos masivos que concentran la mayor parte de los beneficios derivados de la vigilancia masiva y aplicación en el contexto democrático, entre otras cosas**.**

Esta deriva democrática se percibe claramente a través del aumento exponencial de los casos de aplicación de imperativos sistémicos que, como el poder, el dinero, el control y la opinión sintética y artificial son puestos en marcha por los estados y los mercados para controlar y constreñir la actividad de la sociedad civil con fines meramente instrumentales.

No obstante, como se ha intentado mostrar en este estudio, una democracia madura y robusta exige de una sociedad civil fuerte, comprometida y participativa que sea capaz de introducirse y aportar en aquellos procesos democráticos que, como la vigilancia del resto de esferas que componen la democracia, velan por su buena salud y correcto desarrollo. Pero para ello, es necesario abrir espacios de libertad, cooperación y empoderamiento donde la sociedad civil pueda desplegar

su actividad y actuar como contrapoder democrático. Prácticas como el *activismo de datos*, el *hackerismo* ético y el *whistleblowing* son algunas de las actuales capacidades de la sociedad civil para cooperar, empoderarse y postularse como contrapoder del actual escenario de vigilancia masiva basada en datos y metadatos masivos. Las instituciones democráticas tienen el deber de velar por el acontecer y por el conocimiento de los espacios de libertad, cooperación y empoderamiento, puesto que, como afirmó Tocqueville (1990a, b), es condición de posibilidad de una democracia madura de, por y para la ciudadanía.

En suma, este trabajo ha intentado abordar críticamente la emergencia e impactos de un nuevo orden geoestratégico (político y económico) basado en la vigilancia masiva de la ciudadanía y los datos y metadatos que esta produce con el principal objetivo de ofrecer orientaciones sobre cómo capacitar a la sociedad civil para establecer un contrapoder frente a los gobiernos políticos y los mercados económicos de vigilancia.

9. Bibliografía

Apel, K-O. (1985). *La transformación de la filosofía*. Madrid: Taurus.

AppleInsider Staff (2016). "Apple hires firmware security experts who worked on Thunderstrike 2 exploit". *AI*, 03/02/2016. https://appleinsider.com/articles/16/02/03/apple-hires-firmware-security-experts-who-worked-on-thunderstrike-2-exploit. Fecha de consulta: 09/10/2023

Armenteras, D., González, T. M., Vergara, L. K., Luque, F. J., Rodríguez, N., y Bonilla, M. A. (2016). "A review of the ecosystem concept as a "unit of nature" 80 years after its formulation". *Ecosistemas*, vol. 25, n. 1, pp. 83-89.

Bartlett, J. (2018). *The People Vs Tech: How the internet is killing democracy (and how we save it)*. Londres: Penguin Random House.

Boffey, Ph.M. (1971). "Nader and the Scientists: A call for responsibility", *Science*, vol. 171, n. 3971, pp. 549-551.

Caffarena, V. A. (2017). "El valor del activismo de datos en el trabajo de la sociedad civil",*Dígitos*, vol. 1, n. 3, pp. 199-220.

Cave, D., Hoffman, S., Joske, A., Ryan, F., y Thomas, E. (2019). *Mapping China's technology giants* (N.º 15/2019). Sydney: Australian Strategic Policy Institute. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-05/Mapping%20China%27s%20technology%20giants.pdf?EINwiNpste_FojtgOPriHtIFSD2OD2tL. Fecha de consulta: 25/03/2023

Clarke, R. A., Morell, M. J., Stone, G. R., Sunstein, C. R., y Swire, P. (2014). T*he NSA Report: liberty and security in a changing world*. Princeton: Princeton University Press.

Calvo, P. (2016): "*Whistleblowing ante la miseria moral de instituciones y organizaciones", en:* J. V. Meseguer y M. Avilés (dirs.). *Empresa, Derechos Humanos y RSC. Una mirada holística desde las Ciencias Sociales y Jurídicas. Pamplona: Aranzadi Thomson Reuters, pp. 135-153.*

Calvo, P. (2020). "Democracia aumentada. Un ecosistema ciberético para una participación política basada en algoritmos", *Ápeiron. Estudios de Filosofía*, vol. 12, pp. 129-141.

Calvo, P. y Osal, C. (2018). "Whistleblowing y datos masivos: monitorización y cumplimiento de la ética y la responsabilidad social". *El profesional de la información, vol. 27, n. 1, pp. 137-184.*

Conill, J. (2006). Ética hermenéutica. Crítica desde la facticidad. Madrid: Tecnos.

Conill, J. (2008). "Hermenéutica crítica desde la facticidad de la experiencia", *Convivium. Revista de filosofía,* vol. 21, pp. 31-40.

Cortina, A. (1985). "La hermenéutica crítica en Apel y Habermas ¿Ciencia reconstructiva o hermenéutica trascendental?", *Estudios Filosóficos*, vol. 34, n. 95, pp. 83-114.

Cortina, A., García Marzá, D. y Conill, J. (2008). *Public reason and applied ethics. The ways of practical reason in a pluralist society*. New York: Rainer Hampp Verlag.

Cryptoparty (2024). Cryptoparty 2024. https://cryptoparty.ucm.es

Dos Santos, R. (2023). "A mudanca estrutural digital da esfera publica observacoes sobre a atualizacao do diagnostico de Habermas". en: D. J. Volpato y E. Gusmão de Góes (Coords.), *Habermas e a esfera pública: diagnósticos do tempo presente.* Pelotas: NéfilOnline, pp. 406-431.

Emmerson, B. (2015). *Two Years After Snowden: protecting human rights in an age of mass surveillance*. London: Privacy International and Amnesty International.

Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. Washington: Carnegie Endowment for International Pace.

García-Marzá, D. (2013). "Democracia de doble vía: el no-lugar de la empresa en la sociedad civil", *Revista del CLAD. Reforma y democracia,* vol. 57, pp. 67-92.

García-Marzá, D. y Calvo, P. (2024). *Algorithmic democracy. A critical perspective based on deliberative democracy*. Cham: Springer.

Gellman, B., Blake, A., y Miller, G. (2013). "Edward Snowden comes forward as source of NSA leaks". *The Washington Post,* 09/06/2013. https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html. Fecha de consulta: 30/06/2022.

González, C. F. (2021). *El gran sueño de China: tecno-socialismo y capitalismo de estado*. Madrid: Tecnos.

Greenwald, G., MacAskill, E., y Poitras, L. (2013). "Edward Snowden: the whistleblower behind the NSA surveillance revelations". *The Guardian,* 11/06/2013. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Fecha de consulta: 30/06/2022

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* Nueva York: Metropolitan Books.

Gutiérrez, M. (2018). *Data activism and social change*. Cham: Palgrave Hardcover.

Gutiérrez-Rubí, A. (2014). "Hablemos claro ¿y si forzamos la apertura? Protección a los whistleblower, *Actualidad administrativa,* n. 7-8, pp. 864-869.

Habermas, J. (1987). *Teoría de la Acción comunicativa. Vol. II*. Madrid: Taurus.

Habermas, J. (1984). *Conocimiento e Interés*. Madrid: Trotta.

Habermas, J. (1998). *Facticidad y Validez. Sobre el derecho y el Estado democrático de derecho en términos de teoría del discurso.* Madrid: Trotta.

Habermas, J. (2023). *Un nou canvi estructural en l'esfera* pública *i la política deliberativa*. Barcelona: Edicions 62.

Han, B. C. (2021). *Psicopolítica: Neoliberalismo y nuevas técnicas de poder*. Barcelona: Herder.

Hannig, S. (2019). *Distopía Digital: Cuatro herramientas que China utiliza para controlar a su población*. Santiago: Fundación para el Progreso (FPP). https://fppchile.org/distopia-digital-cuatro-herramientas-que-china-usa-para-controlar-a-su-poblacion/. Fecha de consulta: 02/08/2022.

Helberg, J. (2021). *The wires of war: technology and the global struggle for power*. Nueva York: Avid Reader Press.

Hillman, J. E. (2021). *The digital Silk Road: China's quest to wire the world and win the future.* Londres: Harper Collins.

Himma, K. E. (2007). *Internet security: hacking, counterhacking, and Society.* Sudbury: Jones and Bartlett.

Hoffman, S., y Attrill, N. (2021). *Mapping China's Tech Giants: Supply chains and the global data collection ecosystem* (N.º 45/2021). Sydney: Australian Strategic Policy Institute. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2021-06/Supply%20chains.pdf?VersionId=56J_tt8xYXYvsMuhriQt5dSsr92ADaZH. Fecha de consulta: 28/03/2023

Howard, P. N. (2020). *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. Yale: Yale University Press.

Hwnag, T. (2010). "Digital transforms activims: The web ecology perspective", en: M. Joyce (Ed.), *Digital Activism Decoded. The New Mechanics of Change*. Nueva York: International Debate Education Association, pp. 119-136.

Jiang, M., y Fu, K. W. (2018). "Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?". *Policy & Internet*, vol. 10, n. 4, pp. 372-392. https://doi.org/10.1002/POI3.187

Jiménez, R. (2016). El Pentágono quiere contratar háckers. *El País, 02/03/2016.* https://elpais.com/internacional/2016/03/02/estados_unidos/1456956517_636637.html?event_log=oklogin. Fecha de consulta: 08/09/2022.

Joyce, M. (2010). "How to Think About Digital Activism". en: M. Joyce (Ed.). *Digital Activism Decoded The New Mechanics of Change.* Nueva York: International Debate Education Association, pp. 1-14.

Keane, J. (1992). *Democracia y sociedad civil*. Barcelona: Alianza.

Kliman, D., Doshi, R., Lee, K., y Cooper, Z. (2019). *Grading China's Belt and Road*. Washington: CNAS.

La Información (2011). El hacker que desbloqueó el iPhone ficha por Apple. *La Información,* 26/08/2011. https://www.lainformacion.com/economia-negocios-y-finanzas/el-hacker-que-desbloqueo-el-iphone-ficha-por-apple_7zu20ZTSV7QYoi3tJeLo36/. Fecha de consulta: 06/10/2022

La Quadrature du Net (2023). "La france, premier pays d'europe à légaliser la surveillance biométrique". *La Quadrature du Net,* 23/03/2023. https://www.lainformacion.com/economia-negocios-y-finanzas/el-

hacker-que-desbloqueo-el-iphone-ficha-por-apple_7zu20ZTSV7QYoi3tJeLo36/. Fecha de consulta: 23/04/2023.

Labonde, M., Malhuret, L., Piedallu, B. y Simon, A. (2021). *Internet et libertés: 15 ans de combat de la Quadrature du Net*. París: Vuibert.

Lee, K. F. (2020). *Superpotencias de la inteligencia artificial: China, Silicon Valley y el nuevo orden mundial*. Bilbao: Deusto.

Liboiron, M. (2014). "Data activism: Occupy Sandy's canvassing practices after Hurricane Sandy". *Superstorm Research Lab,* 11/08/2014. https://superstormresearchlab.org/2014/08/11/data-activism-occupy-sandys-canvassing-practices-after-hurricane-sandy/. Fecha de consulta: 10/11/2022

Liboiron, M. (2015). "Disaster data, data activism. Grassroots Responses to Representations of Superstorm Sandy". en: J. Leyda y D. Negra (Eds), *Extreme Weather and Global Media*. Nueva York & Londres: Routledge, pp. 145-162.

Lyon, D. (2015). *Surveillance after Snowden*. Cambridge: Polity Press.

Macaskill, E., y Dance, G. (2013). "NSA files decoded: Edward Snowden's surveillance revelations explained". *The Guardian,* 01/11/2013. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Fecha de consulta: 08/06/2022.

Macdonald, F. (2022). "Marseille's battle against the surveillance state". *MIT Technology Review,* 13/06/2022. https://www.technologyreview.com/2022/06/13/1053650/marseille-fight-surveillance-state/. Fecha de consulta: 25/07/2022

Meaker, M. (2022). "La lucha contra la vigilancia de Marsella y el interminable debate sobre la sensibilidad de la IA". *Heaven 32.* https://www.heaven32.com/la-lucha-contra-la-vigilancia-de-marsella-y-el-interminable-debate-sobre-la-sensibilidad-de-la-ia/amp/. Fecha de consulta: 03/09/2023

Milan, S. y Gutierréz, M. (2015). "Medios ciudadanos y big data. La emergencia del activismo de datos", *Mediaciones*, vol. 11, n. 14, pp. 10-26.

Moore, M. (2018). *Democracy Hacked: How Technology is Destabilising Global Politics*. Londres: Oneworld Publications.

Morozov, E. (2018). *Capitalismo big tech ¿welfare o neofeudalismo digital?*. Madrid: Enclave.

Moser, C. (2016). "Pentagon Launches Pilot Project Challenging Hackers to Test Federal Cyber Security". *IGN,* 02/05/2017. https://www.ign.com/articles/2016/03/03/pentagon-launches-pilot-project-challenging-hackers-to-test-federal-cyber-security?fbclid=IwAR1bGx2-G6DFT6o1PXIoY7PWTc3eRMwD-MwCXKusu6Ho8V-8aBM2kiROv4cY. Fecha de consulta: 05/10/2023.

Mueller, T. (2020). *Crisis of Conscience. Whistleblowing in an age of fraud*. Londres: Penguin.

Nader, R., Petkas, P., Blackwell, K. (Eds.) (1972). *Whistle Blowing*. Nueva York: Bantam.

Nicolás, J. A., Domingo, A., y García-Marzá, D. (Eds.) (2023). *Hermenéutica crítica y razón práctica. Homenaje a Jesús Conill*. Granada: Comares.

Pwnie Award (2023). The 2022 Pwnie Awards Nominations. https://www.pwnie-noms.live

Reigadas, N. (2022). "Si atacan las cámaras de seguridad del Casco Antiguo es porque funcionan". *Hoy,* 18/05/2022. https://www.hoy.es/badajoz/atacan-camaras-seguridad-20220518210356-nt.html. Fecha de consulta: 14/07/2023

Ryan, F., Cave, D., y Xu, V. X. (2019). Mapping more of China's technology giants (N.º 24/2019). Sydney: Australian Strategic Policy Institute. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2019-12/Mapping%20more%20of%20Chinas%20tech%20giants.pdf?VersionId=wpDVHIKgXJHzeK8rZ.kmy0Ei63RxXMO. Fecha de consulta: 28/03/2023

Sampedro, V. (2014). *El cuarto poder en red. Por un periodismo (de código) libre*. Barcelona: Icaria.

Sastre, P. y Gordo, A. J. (2019). "El activismo de datos frente al control algorítmico. Nuevos modelos de gobernanza, viejas asimetrías", *IC: Revista Científica de Información y Comunicación*, vol. 16, pp. 157-182.

Saura García, C. (2023). "El big data en los procesos políticos: hacia una democracia de la vigilancia", *Revista de Filosofía*, vol. 80, pp. 215-232.

Saura García, C. (2024). "Digital expansionism and big tech companies: consequences in democracies of the European Union", *Humanit Soc Sci Commun,* vol. 11, n. 448.

Semenzin, S. (2017). "Hacktivismo y ética hacker: el caso del cryptoparty". En: R. Cotarelo y J. Gil (Eds.), *Ciberpolítica. Hacia la cosmópolis de la información y la comunicación*. Madrid: INAP, pp. 618-642.

Shahbaz, A. (2018). *The Rise of Digital Authoritarianism*. Washington: Freedom House.

Snowden, E. (2019). *Vigilancia Permanente*. Barcelona: Planeta.

Stallwood, O. (2013). "Game to destroy CCTV cameras: vandalism or valid protest?". *The Guardian,* 25/01/2013. https://www.theguardian.com/theguardian/shortcuts/2013/jan/25/game-destroy-cctv-cameras-berlin. Fecha de consulta: 05/06/2023.

Syeed, N. (2017). "Pentagon Hires Hackers to Target Sensitive Internal Systems". *Bloomberg,* 13/02/2017. https://www.bloomberg.com/news/articles/2017-02-13/pentagon-hires-hackers-to-target-sensitive-internal-systems?leadSource=uverify%20wall. Fecha de consulta: 29/09/2023.

van Dijck, J. (2014). "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology", *Surveillance & Society,* vol. 12, n. 2, pp. 197-208.

Vandekerckhove, W. (2006). *Whistleblowing and organizational social responsibility: A global assessment.* Nueva York: Ashgate Publishing Ltd.

Vaughn, R. G. (2020). *The Successes and Failures of Whistleblower Laws*. Northampton: Edward Elgar Pub.

Violaine (2019). "Un logiciel pour décoder les *émotions* des usagers du tramway de Nice". *ICI. Par France Bleu Et France 3,* 04/01/2019. https://www.francebleu.fr/infos/societe/un-logiciel-pour-decoder-les-emotions-des-usagers-du-tramway-

de-nice-1546621455. Fecha de consulta: 06/09/2023.

Webb, A. (2021). *Los nueve gigantes: cómo las grandes tecnológicas amenazan el futuro de la humanidad.* Madrid: Península.

Woolley, S., y Howard, P. N. (Eds.) (2018). *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford: Oxford University Press.

Woolley, S. (2023). *Manufacturing consensus: understanding propaganda in the era of automation and anonymity*. Yale: Yale University Press.

Zuboff, S. (2020). *La era del capitalismo de la vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder.* Barcelona: Paidós.