ANONIMATO, TRANSPARENCIA E IDENTIFICACIÓN DE FUENTES, INFORMANTES Y ROBOTS EN LA ERA DEL ALGORITMO[1]

Loreto Corredoira*

No sé si ustedes conocen las hazañas del general romano Cincinnatus (s. V a.C).
Yo no conocía los detalles hasta hace poco.
Cincinnatus fue el alias elegido por Snowden en 2013
para comunicarse con los periodistas a los que filtró datos y documentos
sobre las actividades de sobrevigilancia de la NSA.
Snowden utilizó ese apodo porque dicho general,
una vez que impidió una invasión de Roma, se retiró a la vida privada,
rechazando las posibilidades de mantenerse en el poder.

1 Este trabajo es parte del Proyecto SN-Disorders (2020-2023) financiado con referencia Proyecto/AEI/10.13039/501100011033 que codirijo, así como del Proyecto de Fondos Next Generation (2022-2024) denominado CYBER-ELECTIONS que codirigen Rafael Rubio y José Mª Coello de Portugal.

* Profesora Titular de Derecho de la Información y *Jean Monnet Chair*, Universidad Complutense de Madrid.

I. INTRODUCCIÓN. EL CAMBIO DE PARADIGMA EN FUENTES INFORMATIVAS

Me preocupa que nos quedemos sin fuentes precisamente cuando más las necesitamos, declaraba Edward Snowden en una entrevista publicada el 30 de julio de 2018 en *Süddeusthe Zeitung*. Este periódico es una de las cabeceras que forma parte del consorcio de noticias International Consortium of Investigative Journalists (ICIJ) con base en Estados Unidos, que une a más de 100 medios y a 280 reporteros del mundo entero. Consorcio que trabaja de forma colaborativa en investigaciones de gran escala transnacional.

Se comparta o no lo que Snowden hizo, las revelaciones de su papel como agente de la CIA, trabajando para la agencia nacional estadounidense de seguridad, la National Security Agency o NSA, se trató de un caso escandaloso de vigilancia masiva que ha supuesto un antes y después en varios asuntos que trataremos en estas páginas: la cuestión de la información pública y su veracidad, la atribución de las fuentes cuando son anónimas, la protección de los informantes y por supuesto del uso de las redes. El de Snowden es un modo de proceder de algunos de los "filtradores" o "informantes" que saben lo arriesgado de su acción. Contravenir el secreto oficial en el ámbito público –caso NSA– o, la confidencialidad en el privado –como la de los documentos bancarios desvelados por Falziani o los informes sobre empresas en *offshores* revelados en los Panamá Papers o los del Russia archive también del consorcio ICIJ–, son razones para buscar el anonimato o la preservación de la identidad con los medios.

Estas fuentes que acuden a la filtración para la denuncia pública de hechos graves, objetivos y probados por supuestos de corrupción o de abuso de poder, están cambiando la formación de la opinión pública y las relaciones clásicas de medios y fuentes informativas. También para los periodistas que tienen un deber de confidencialidad con sus fuentes; es el secreto profesional que además en España y en muchos países occidentales es un derecho constitucional para garantizar las fuentes y el derecho del público a la información. La reserva y protección de las fuentes es además de un derecho constitucional, recogido en España en el art. 20 de la Constitución, un deber ético y profesional (Moretón, 2014: 121-144).

Nos encontramos pues ante dos cuestiones: una la proliferación de denuncias de informantes –expresión por cierto que prefiero frente a la anglosajona

whisteblowers, literalmente los que silban o soplones– que llegan a las redacciones de los medios y a las redes sociales y, dos, la de determinar quién es el titular o emisor de la información en casos como los citados en los que el anonimato es sagrado. Esta es una de las grandes preocupaciones que tienen en la actualidad el periodismo, señalada también por los investigadores o expertos en transparencia (Troncoso, 2021), y por juristas, preocupados por las garantías de los derechos fundamentales. En esa línea y, para facilitar que fluya la información sobre casos de corrupción, la Unión Europea ha planteado la Directiva (UE) 2019/1937, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, para la protección de ese tipo de fuente, que está en proceso de incorporación al Derecho español. De lo que se ha analizado en fase de anteproyecto hasta hoy, las voces de expertos y activistas expresan preocupación pues ese borrador de la futura ley no lleva consigo la modificación del Código Penal que castiga la revelación de secretos, ni establece excepciones para periodistas y fuentes, que sería lo propio.

Como ha destacado Arancha Moretón: "la función informativa consiste en trasladar al público información veraz de relevancia social y, el deber de custodiar la información y la restricción de su publicidad es un deber que recae, en la propia Administración de Justicia". En este sentido hay, sin duda conflictos, y puede hasta resultar imposible la protección de información secreta y confidencial merced al secreto profesional constitucional. Recuerda Moretón varios casos de filtraciones que han llegado ante el TEDH de Estrasburgo, destacando "el Caso Fressoz y Roire vs. Francia, recurso núm. 29183/95 (Sentencia del 21 de enero de 1999), donde se pone de relieve que la conducta de los informadores que publican documentos con datos fiscales proporcionados por funcionarios violando su deber de reserva (es decir, de manera ilícita) *no constituye per se un ejercicio ilegítimo del derecho a la información*, de manera que la licitud o no de su conducta ha de valorarse teniendo en cuenta otros criterios como, por ejemplo, el interés público de la noticia, su veracidad, la posibilidad de obtener esa información por otros medios, etc., sin que deban asumir responsabilidad alguna por no identificar a quienes les hubieran filtrado esos documentos (con independencia de la eventual responsabilidad de quienes los hubieran filtrado) (Moretón, 2014: 18)".

Ante el crecimiento de las noticias falsas y, sobre todo, ante la falta de "acreditación" o "atribución" de la verdad o falsedad de distintos "ciberincidentes",

comparto lo que afirmaba Snowden a los reporteros alemanes: ahora las fuentes son más importantes que nunca. Tanto las fuentes periodísticas tradicionales, si se puede seguir diciendo así, como las derivadas de las tecnologías, que permiten tanto el anonimato de quien filtra (a modo de Cincinnatus) como una entrega masiva de datos.

Las llamadas "fuentes disruptivas" en el periodismo han modificado las rutinas de las redacciones planteando problemas que analizaremos aquí (Wasserman, 2016). De hecho, el Consorcio ICIJ antes citado, define su actividad como un equipo masivo de periodistas trabajando de forma colaborativa tanto en tratamiento de datos como en análisis periodístico de la información, tarea que un medio por sí solo no puede conseguir. Así se presentan:

> *By gathering massive teams of journalists from all over the world to work together on major investigative projects, ICIJ is able to expose the faults in national and international institutions that are supposed to protect us – but too often are failing. By working together, we can achieve results and impact that no single outlet could achieve on its own, and we can provide citizens around the world with the knowledge they need to hold the powerful to account. We consider ourselves global leaders in data journalism and journalism technology. Our digital innovations, our secure international network and our access, through whistleblowers, to gigantic data sets that exist nowhere else, allow us to dig out information that would otherwise be hidden from view.*
>
> *We are both a small, resourceful newsroom with our own reporting team, as well as a global network of reporters and media organizations who work together to investigate the most important stories in the world.*

Este ejemplo muestra además el cambio en las relaciones de poder, acciones como las descritas permiten investigaciones más ambiciosas que medios locales no podrían asumir por coste y por la pericia técnica necesaria. Dicho cambio se debe por una parte a una mayor la participación del público en redes, a la difusión y facilidad de acceso a la información y, por otra, a que las máquinas y su lenguaje o *software* (los algoritmos) están introduciendo otras variables en el flujo de comunicación clásico. Una de ellas precisamente es la autoría o atribución, es decir la identificación del emisor o fuente y por otra, su veracidad o autenticidad que trataremos en este capítulo.

II. DE RATONES (RO-BOTS) Y DE HOMBRES. PROBLEMAS DE TRANSPARENCIA ANTES FENÓMENOS DE ESPIONAJE Y DESINFORMACIÓN A GRAN ESCALA

Elegí el título de la película "De ratones y de hombres" al pensar en el título de este apartado, no por sintonía de la novela de Steinbeck, sino por la cacofonía de "robots y de hombres" con la que quiero jugar, al tratarse de una realidad tan mediatizada por las "tecnologías". En este punto afronto pues varias cuestiones, algunas de ellas parten de investigaciones en marcha de las más importantes en Europa en los últimos veinte años sobre la red, transparencia, libertades, etc. en las que he participado junto a otros colegas de este libro y de los proyectos de investigación en marcha, Cotino, Rubio, Boix, Serrano, Moretón, Arellano, entre otros.

Para poner esta investigación en su contexto y calibrar el cambio de paradigma social, hemos de decir que estamos "emigrando" desde un mundo de Estados fuertes, típicos de la guerra fría posterior a la II guerra mundial, a otro mundo de Estados debilitados, con potentes empresas o conglomerados de tecnología que han incorporado la "vigilancia" no sólo como control sino como método de influencia y de rentabilidad económica.

Dicha rentabilidad se basa en una materia prima, el nuevo petróleo del *big data*, con el valor añadido de la Inteligencia Artificial y de, en muchos casos, su utilización torticera por agencias de relaciones públicas y plataformas tecnológicas. De hecho, autores como Zuboff (2020), hablan del "capitalismo de la vigilancia" en el mundo libre, frente al control férreo de Estados o gobiernos no transparentes cuando no despóticos.

Siendo distintos los supuestos que vamos a ir analizando, unos de filtraciones, otros de campañas de desinformación; unos con clara dirección humana y otros con intervención y cierto descontrol algorítmico, tienen en común que son verdaderos jaques a los Estados democráticos, alterando a veces la paz social, cuando no algunos procesos electorales. En lo que a este trabajo se refiere, comparten además no sólo el tratamiento masivo de datos, sino la pericia para su acceso o incluso robo, cuando no la filtración.

La irrupción de las redes sociales en la primera década de este siglo XXI presenta más vulnerabilidades en derechos fundamentales como la intimidad,

traspasa los límites de la propiedad, que se ha visto asaltada por dispositivos de grabación, captación de imágenes y sonido.

Comparto con Han (2021) que la vigilancia se ha privatizado, con la anuencia de todos nosotros, usuarios híper-conectados a las redes. Idea que confirman otros autores, como Wylie matemático del análisis cualitativo de la información en *Cambridge Analytica*, en su calidad de exdirectivos de empresas que han colaborado en filtraciones de abusos de datos. Wylei llega a decir que "Facebook ya no es solo una empresa. Es un monopolio (...) una amenaza para la Seguridad Nacional", alertando de que "no saben qué hacer con tanta información" (Wylie, 2020: 32). Wylie, ya arrepentido, fue precisamente la fuente anónima de la periodista Carolle Cadwalladr del diario británico *The Guardian*, periodista y medio que más tiempo e investigación dedicaron a esta cuestión, como fueron publicando con todo detalle en 2017.

Casos recientes como las filtraciones de Facebook en la "trama rusa" de los EEUU muy bien documentado por David Alandete (2021), corresponsal del ABC Washington, no son totalmente desconocidas para el lector. Las injerencias en el "conflicto catalán" han sido más que documentadas por Del Fresno y Manfredi en trabajos científicos bastante únicos, y por supuesto han ocupado a las Fuerzas y Cuerpos de Seguridad, también al Poder judicial en casos como Volhof[2] ahora abierto en el Juzgado de instrucción nº 1 de Barcelona con motivo de las escuchas del *software Pegasus* a independentistas catalanes.

También el Parlamento Europeo (2020) se ha sumado con una posición clara, sobre el asunto de la injerencia extranjera y maliciosa en procesos electorales, alertando del riesgo de maniobras de intervención en la comunicación pública.

III. VIGILANCIA MASIVA POR PARTE DE LAS GRANDES DE TECNOLOGÍA

Respecto a la colaboración de grandes plataformas como Facebook en determinados métodos de perfilado de publicidad política y de obtención de datos, el escándalo ha sido inmenso, sobre todo porque veníamos alertados

2 El juez imputa al supuesto espía ruso que ayudó al círculo de Puigdemont https://www.elmundo.es/cataluna/2022/04/27/62696afae4d4d8ae4d8b4598.html

por Snowden (Snowden, 2021) del "colaboracionismo" de Google y las telecos de EEUU con la NSA. Que lo hiciese la NSA se podía comprender pues al fin y al cabo son una agencia pública de inteligencia y de espionaje y sus acciones podría tener un cierto amparo legal en sus investigaciones –que por naturaleza, claro, son secretas y con poco control de otros poderes del Estado–, pero, la vigilancia masiva a todo tipo de ciudadanos y el uso de datos de los usuarios de las grandes plataformas de EEUU (Facebook, Google, Amazon) con fines privados, políticos o comerciales ha sido excesivo. Especialmente por venir del país que consideramos libre y democrático por excelencia pero que en términos de protección de la privacidad deja mucho que desear.

Facebook entró además en la lógica de los estrategas de *Cambridge Analytica* para el perfilado y discriminación de los usuarios, aun cuando esto suponía el robo y obtención ilegítima de datos personales (el petróleo, les recuerdo). Steve Banon, estratega electoral muy discutido, vio el gran potencial del micro-perfilado de los usuarios y lo aplicó al discurso público en Estados Unidos (Wylei, 2020: 27).

Lo que conocíamos sobre la colaboración de Facebook –hoy rebautizada como Meta– ha ido empeorando por la filtración y comparecencias públicas de la ex directiva Frances Haugen en noviembre de 2021 en el Parlamento Europeo[3] como lo hiciera antes en el Senado de los Estados Unidos. Sus declaraciones ponen de manifiesto que hay conductas que no pueden exonerarse sólo por "fallos técnicos" o errores de alcance, y que deben ser exigibles ética y jurídicamente. Zuckerberg escribía esto en un post después del escándalo Facebook *"There's more we can do here to limit the information developers can access and put more safeguards in place to prevent abuse*" tras haber comparecido en el Senado Americano en abril de 2018. La sinceridad de esas palabras del fundador del hoy llamado *Metaverso* es discutible después de haberse conocido sus métodos con más detalle.

Por tanto, en este primer nivel de análisis de las garantías de transparencia y libertades, ponemos la atención en los riesgos de acciones de vigilancia, espionaje y desinformación de gran escala: algunos urdidos sólo por humanos

3 Publicado el video completo de su intervención ante el Committee on the Internal Market and Consumer Protection https://multimedia.europarl.europa.eu/en/webstreaming/imco-itre-juri-libe-inge-aida-econ-joint-hearing_20211108-1645-COMMITTEE-IMCO.

y otros con la colaboración de las matemáticas, la Inteligencia Artificial y la velocidad de las redes y ordenadores que utilizamos.

Como ha afirmado la Comisión Europea, "la exposición de los ciudadanos a la desinformación a gran escala, incluida la información engañosa o directamente falsa, es un reto importante para Europa" (2017). Alertaba ya entonces la Comisión no sólo de la difusión a gran escala de información "engañosa" sino también de la "totalmente falsa". Algo que en 2022, durante la invasión de Ucrania por Rusia, se ha visto incrementado. Tanto que la UE ha decidido prohibir, en una decisión sin precedentes, la distribución de señales de "radiodifusión", incluyendo el *streaming,* a los canales RT y/o Sputnik. El argumento literal del Consejo, que sigue en vigor al cierre de este libro, fue que *such actions constitute a significant and direct threat to the Union's public order and security* (Reglamento del Consejo Europeo de 1 de marzo de 2022); la amenaza se consideró directa y grave contra el "orden público y la seguridad".

Así lo explicaba Josep Borrell, Alto Representante de la UE, pocos días después en el Parlamento Europeo: "hay que combatir esta narrativa, primero, cortando las fuentes de desinformación, como hemos hecho. Y después hay que desarrollar la nuestra. Porque no basta con silenciar la suya, hay que desarrollar la nuestra. Y les invito a todos ustedes, parlamentarios, que desarrollan una gran labor de diplomacia parlamentaria, a hacerlo ahora, más que nunca, llevando la voz de Europa para explicar qué es lo que realmente pasa. Porque no todo el mundo tiene la misma clara conciencia que nosotros sobre lo que está pasando en Ucrania. Los mensajes falaces trucados de mentiras pueden perfectamente contaminar las mentes de aquellos que no tienen más información que la que reciben. Es nuestra obligación dar esa información permanentemente, porque tenemos una batalla acerca de la interpretación histórica de estos acontecimientos".

Esto indica el paradigma geopolítico de la cuestión que a mi entender supone un giro importante en la neutralidad y moderación de la UE en estos últimos años, sentando un peligroso precedente. Desde la guerra fría entre la URSS y occidente, no veíamos acciones coordinadas de bloqueo de emisoras de radio o televisión con tanto alcance como éste. Entonces se prohibía la distribución de radios o televisiones libres, hoy se imponen medidas de bloqueo a las empresas de Internet que están en la jurisdicción europea.

El tema no es sencillo y nos ocupará probablemente mucho a los constitucionalistas y autores del Derecho de la Información, pero también hay que decir que no es totalmente nuevo, el bloqueo de páginas web o canales de video, se ha hecho en nombre de la "propiedad intelectual", eliminando servidores o blogs e, incluso las propias plataformas como YouTube, han borrado o bloqueado contenidos cuando les ha parecido oportuno, sin garantía judicial alguna.

Esta situación de control de las llamadas "narrativas hostiles" a través del cierre de medios en Europa, si se prolonga, es constitucionalmente dudosa en un continente que ha dado a luz a dos grandes declaraciones de derechos humanos. En otra investigación que nos ocupa en el Observatorio Complutense de la Desinformación[4], consideramos clave definir si tanto RT como Sputnik son o no medios, o si son más bien panfletos y si, en consecuencia, les alcanza la protección del derecho a la información veraz o no. Por cierto que en España RT está pudiendo emitir desde sitios como *VT.com/Rt_internationalhttps://vk.com/rt_international*.

IV. *BIG DATA, BIG PROBLEMS*

Así pues, en este contexto de información pública y de vigilancia estatal, el espionaje político, diplomático e industrial de eras pasadas en el siglo XX, se ha convertido en la actualidad en un gran hermano privado, evidenciando la vigilancia masiva que casos como NSA o Facebook-*Cambridge Analytica*, permite pensar que en expresión de Faifield y Shtein que el *big data* se haya equiparado a *big problems* en el campo del Derecho y la ética de la tecnología (Fairfield and Shtein, 2014: 38-51).

Sin duda, en este panorama que se ha esbozado preocupan las garantías de los derechos concernidos, por la importante amenaza de la vigilancia pública y privada, en especial el derecho a la información y la libertad de expresión, el acceso a Internet y los derechos al honor, intimidad, datos y vida privada. Este es el quid del asunto que nos ocupa a los que estamos en la academia: dotar de nuevas garantías a los usuarios, a los ciudadanos e instituciones en una sociedad tan tecnologizada (Cotino, 2017).

4 Observatorio disponible en la URL: observatoriodesinformacion.ucm.es.

La mecanización de los procesos, los algoritmos como modo de personalización de la información o el perfilado de las ofertas publicitarias, hace que la información que recibimos sea más "certera" especialmente gracias a los teléfonos y otros dispositivos móviles que manejan casi el cien por cien de la población, incluso en países del tercer mundo. Siguiendo con las metáforas de recientes series de televisión: en el ámbito de la producción de medios digitales estamos "cambiando" de los *Madmen*, popular serie de 2007, a *Mathmen*, siendo hoy más importante o valorada la astucia y el cálculo matemático que la ideación de extraordinarias campañas de publicidad. El nuevo perfil de los publicitarios y expertos de las empresas requiere científicos de datos, matemáticos y hasta filólogos (Junco, 2022).

La industria de la comunicación tradicional y digital ha incorporado además las llamadas *programmatic ads*, la publicidad automatizada en las web y aplicaciones que reemplazan decisiones humanas estratégicas en la gestión de anuncios. Toda una cuestión que puede hacer desaparecer un sector de intermediación tradicional entre medios y empresas. Y esto pasa no sólo en lo comercial, también en lo político y en lo periodístico. Como han sostenido Cetina y Martínez-Sierra (2019) y Hermida (2017) el "algoritmo se ha convertido en editor".

V. PROBLEMAS DE TRANSPARENCIA DE LOS MENSAJES Y AUTORES EN REDES. AUTENTICIDAD Y ATRIBUCIÓN

Además de lo dicho en el punto anterior, en la llamada "era de la posverdad", en la que todo se cuestiona (Bel, 2021), la comunicación pública se ve interferida y perjudicada por varios problemas. Por un lado, por alteraciones de las fuentes como las antes mencionadas; unas por disrupción de nuevos informantes, otras por la rápida difusión de determinadas investigaciones, lo que acarrea falta de precisión o exactitud. Por otro, por fenómenos automáticos programados, acelerados por el uso de *bots*, robots, vamos, y *trolls*, versiones sencillas del *machine learning* (aprendizaje automático) o del uso de la Inteligencia Artificial que puede ser aún más sofisticada.

Una de las grandes cuestiones jurídicas sobre los humanos y máquinas que ahora nos importa considerar en relación con la transparencia y autenticidad especialmente del periodismo en redes, es la siguiente. En la generación de

información de valor (noticias, publicidad o ideas) para dar veracidad a una fuente –por tanto al periodista y al medio–, hay que estudiar e identificar bien al autor, lo que puede variar si se hace por medio de personas o en colaboración con la tecnología. Por ejemplo, si la portada de un diario la decide no sólo el editor de portada sino un sistema robotizado en función de la relevancia o clics de las noticias. En mi opinión, la clave es la identidad en dos sentidos; en el de origen o fuente y en el de autoría o atribución –en este segundo caso quiere decir autor material o informador–.

Respecto a la autoría u origen de la información y fuentes, en principio las reglas del periodismo, sea impreso o en línea son o deben ser las mismas: el profesional es el que firma la noticia o reportaje, el fotógrafo, el editor o productor de una pieza de televisión o radio, etc. Normalmente las noticias o reportajes o columnas de opinión van firmadas con nombre, aunque pueden ir con seudónimo o incluso de forma anónima. Si ha preocupado en estas últimas décadas la generalización de una práctica en medios que es "no firmar", a veces porque el medio no deja al periodista –sobre todo porque los derechos de autor van al patrimonio común del medio y no de la persona–, apareciendo firmas como "Local", "Sección Nacional", etc. Eso puede resultar también esquivo ante el problema de la transparencia de la información: siempre es mejor firmar y que se identifique el responsable de la noticia en condiciones normales en una sociedad. Solo cabe una excepción importante: la de aquellos países donde el ejercicio del periodismo suponga el señalamiento de periodistas e incluso la muerte. Sin entrar ahora en más detalles, eso afecta también a otras cuestiones sobre quién responde, cómo se pide una rectificación, quien cobra los derechos remuneratorios de propiedad intelectual, etc.

El tema de la identidad en red puede ser más complejo que en el papel. Ya no nos referimos a quién firma sino al perfil o identidad (ID) de quién o qué medio pública. Normalmente una dirección IP (el número de *Internet Protocol*) es igual a una persona o medio y, por tanto, a un usuario o ID. Sea en Twitter, Facebook, Instagram, TikTok o YouTube: todos aparecemos con una ID, identidad que hemos elegido dentro de las peculiaridades de lo que deja la red. Salvo usuarios muy expertos que utilicen siempre una red virtual (VPN) o un navegador encriptado (tipo TOR), el común de los usuarios es fácilmente identificable.

En este sentido y para identificar a los usuarios, algunas redes han ido cambiando sus políticas de uso y ya no permiten que un mismo correo electrónico[5] tenga más de un perfil en la red. En general se pide un registro que incluye teléfono –a veces con una combinación de claves para mayor seguridad–, lo que sin duda es una práctica razonable, y cuando somos un usuario corriente de las redes, facilita la gestión del día a día y la responsabilidad. Si, además, el usuario es un menor –de 13 años en Google–, pasa a ser una "cuenta supervisada" por un adulto, por tanto con doble proceso de identificación.

Algunas redes como Twitter aportan el dato de "usuario verificado", con mensajes como *esta cuenta está verificada debido a que tiene notoriedad en el ámbito gubernamental, de noticias, entretenimiento u otra categoría designada"*, y remiten a su política de "Verificación de cuentas"[6] que cualquier usuario medio puede pedir si quiere ser más creíble en redes o evitar plagios o suplantaciones. Tema que se ha replanteado con la reciente compra de la red por Elon Musk.

Sin embargo, cuando se manejan varias cuentas o cuando –como diremos– se genera una campaña falsa –mediante *astroturfing*, *bots* o sistemas mecanizados en una agencia de comunicación digital–, las confusiones son más que posibles. Son incluso intencionadas. Cualquiera de nosotros tenemos experiencias de lo complejo que es utilizar una aplicación o servicio en nube si no nos hemos autentificado, identificado, en un ordenador habitual. A nivel corporativo o de comunicación a gran escala –como las campañas de publicidad o de propaganda electoral– se acude de forma organizada y eficiente a la gestión mecánica de varios *bots*[7], *trolls*[8], máquinas, que emulan a varios incluso miles de usuarios, sin necesidad de "cambios" de correo con el fin de amplificar una campaña. Ahí precisamente es donde se difumina quién es el autor y emisor.

---

5 Véanse, por ejemplo, las indicaciones de Google para Youtube o Gmail. https://support.google.com/youtube/answer/174100?hl=es.

6 Véase https://help.twitter.com/es/managing-your-account/about-twitter-verified-accounts.

7 En Diccionario de la RAE. Del ingl. *bot*, acort. de *robot* 'robot'. "Inform. robot (programa)".

8 Definido también por la RAE como proveniente del noruego *troll* 'ser sobrenatural'. "En foros de Internet y redes sociales, usuario que publica mensajes provocativos, ofensivos o fuera de lugar con el fin de molestar, llamar la atención o boicotear la conversación".

La transparencia en el sentido de identificación de quién es quién en las redes que se exige en el Derecho de Internet, básicamente las normas de la corporación internacional de gobierno de Internet (ICANN), es la identificación de la IP o dominio de una web o sitio y la de su administrador.

Desde el otro lado de la red, cuando lo que se exige es la identificación o transparencia de un usuario, el tema es delicado, no hay justificación para exigir el uso del DNI o pasaporte en red, pues el anonimato en cierto modo parte del derecho de acceso que implica la no discriminación y del derecho a la intimidad en las comunicaciones. Y, aunque no se ha incluido como derecho digital en la última reforma de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), sí se menciona el *pseudoanonimato* en la Carta de Derechos Digitales de 2021[9].

Cabría pensar en excepciones si hablamos de menores o de circunstancias excepcionales para evitar desórdenes de desinformación, falsedad o acoso. Para esto segundo todavía queda mejorar el proceso de verificación de menores, pues en general los métodos para verificar la edad son más que discutibles.

En los casos en que esa comunicación que no está identificada es intencionadamente maliciosa, estará diseñada para confundir y manipular, y a esos *bots* –como es habitual– se suma la acción de *trolls*, es decir, humanos para lograr una alteración de la conversación aún mayor. Y, además, en este supuesto sí que la transparencia respecto a la fuente, origen etc., es inexistente.

En redes vemos a diario perfiles de profesionales independientes como Mariluz Congosto (@congosto) o Javier Barriuso (@Barri) en Twitter que desentrañan campañas tejidas con máquinas, creando falsos ecosistemas informativos, con *trolls*, *influencers* y *software*. Un ejemplo reciente: Mariluz Congosto que delata la reaparición de un "*troll* que reaparece" con este texto:

9 Promovida por el Gobierno de España y disponible: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (*visitado el 30 de septiembre 2022*).

El troll Ana Guderian ha vuelto. Ahora se llama ana_guderian_ y es pro-ruso. Hace unos años apoyaba el procés de esta forma y los que lo difundían eran estos: https://twitter.com/congosto/status/1054084585103998978… Voy a ver cuáles son los de ahora. Fuente: @congosto, Twitter. 2/5/2022.

Así que, podemos concluir que, especialmente en crisis informativas y en campañas electorales, la presencia de ro-bots en la información en redes, también en el periodismo está alterándolo todo y es un campo en que nos jugamos mucho en las sociedades democráticas.

Algunos trabajan desde agencias de relaciones públicas, no son necesariamente ingenieros informáticos muy expertos, sino que están en despachos donde se prepara esa estrategia de *astroturfing* para "imponer artificialmente movimientos ciudadanos o tendencias de opinión, estrategia que pervierte la autenticidad del termómetro social" (Anónimo, 2022: 14), afirmación del autor/es de ese libro cuya autenticidad está discutida.

Tampoco debemos dejar de decir que, además de en campañas electorales o de reputación política, el uso de *bots* o *trolls* es una práctica habitual en los programas de telebasura, concursos mediáticos donde las audiencias importan más que nada; de ahí que se creen *trending topics* desde por la mañana para generar tráfico, reputación, ataques a la reputación o simplemente ruido.

No nos detenemos más porque el libro que tienen entre manos afrontará más cuestiones sobre la IA; los robots o máquinas con aprendizaje cuasi humano (*machine learning*), entre otras realidades de la "inteligencia artificial" intervienen también en el periodismo y en la comunicación de la esfera pública de ahí que afecten a la sociedad y a la democracia.

VI. APUNTES DE SOLUCIONES ÉTICAS Y JURÍDICAS PARA LA MEJORA EN TRANSPARENCIA DE FUENTES, GARANTÍAS DE LIBERTADES Y AUTENTICIDAD

Como decía esta realidad que hemos descrito tan *tecnologizada,* exige un esfuerzo académico y también de auto y co-regulación en la transparencia específicamente en las redes sociales, con el fin de mejorar la autenticidad de las fuentes: tanto sobre quién emite como de su contenido.

A nivel teórico sin duda, debemos partir del trabajo sobre la transparencia radical que Han critica pues presenta situaciones críticas para determinados derechos y en el contexto de este trabajo, en especial es aguda la falta de veracidad, pues "transparencia y verdad, afirma no son idénticas" (Han, 2019: 22). Concepto que es más amplio que el de transparencia y acceso a la información pública, que tienen su origen en los países escandinavos en los años 70, y que han ido cristalizando en leyes de transparencia y en autoridades para su vigilancia y control.

Llegamos pues al punto en que se deduce claramente que la trasparencia "documental" o de "fuentes" (el derecho de "acceso a la información") necesita ser complementada por la algorítmica, entendiendo ahí todo proceso automatizado, como garantía de los principios de participación, gobernanza y respeto a las libertades informativas.

Entre las tendencias que se apuntan como soluciones quisiera destacar:

a) La necesidad de una nueva política de gobernanza de Internet que contemple más transparencia, por supuesto, con medidas frente a la desinformación e interferencias como ha destacado Divina Frau-Meigs en las soluciones aportadas para un mejor cumplimiento o *compliance* (2021: 144), pero también, en expresión de la Dra. Farzaneh Badii, Directora ejecutiva del *Internet Covernance Project* (IGP) con disposiciones sobre la "atribución pública" de los "ciber-incidentes"[10].

Estas exigencias de transparencia proceden de diversas fuentes o ámbitos del Derecho: el debido proceso, que va más allá del derecho de acceso a la información pública, la vida privada y el derecho a la protección de datos e incluso nuevos derechos fundamentales; también del ámbito de la política pública y la gobernanza. Y como se estudia en este libro, no son pocas las barreras a la transparencia algorítmica: la naturaleza de "caja negra", la opacidad en el diseño, la propiedad y valor de los mismos datos, etc.

10 Véase el New IGP White Paper: Is It Time to Institutionalize Cyber Attribution? Disponible en https://www.internetgovernance.org/2018/08/21/new-igp-white-paper-is-it-time-to-institutionalize-cyber-attribution/ (visitado el 30 de septiembre).

"Quien crea, afirma Han, que transparencia es sólo lucha contra la corrupción y libertad de información, desconoce su envergadura. La transparencia es una coacción sistémica que se apodera de todos los sucesos sociales y los somete a un profundo cambio" (Han, 2021: 12), teniendo todos claro que "la hiperinformación no añade necesariamente luz" (Han, 2021: 80).

Llegamos pues al punto en que se deduce claramente que la trasparencia "documental" o de "fuentes" (el derecho de "acceso a la información") necesita ser complementada por la algorítmica, entendiendo ahí todo proceso automatizado, donde comparezcan como garantías los principios de participación, gobernanza y respeto a las libertades informativas.

b) *El surgimiento de políticas que introduzcan sistemas de "accountability" o "rendición de cuentas".* Precisamente ahora que la ética o, la falta de ella, es más rebuscada, esas políticas deben ser medibles y "vigiladas" también porque son muchos los interesados en procesos electorales, de información económica, o incluso en la Universidad.

Por un lado, como se ha dicho, se trata de un proceso en el que intervienen muchos agentes en Internet, es el llamado *multistakeholderismo* (Pisanty, 2007), o la citada ICANN (Corporación para la Asignación de Nombres y Números en Internet)[11] de la que se han hecho abundantes estudios en los últimos 25 años con libros básicos de varios autores como Arellano 2017, Cotino y Corredoira, 2013, García Mexía 2009, para ver los primeros pasos del Derecho y Políticas de internet[12].

c) Se requiere hoy a las instituciones públicas y privadas *un cumplimiento o compliance* (entendida como "conformidad lega") para incrementar la confianza social, como dijera hace décadas Kelman (1958) o, más recientemente, Simmons (1998). Son requisitos básicos para el cambio.

11 Véase en concreto cómo funciona dicha institución en https://www.icann.org/resources/pages/newcomers-2015-04-01-es.

12 Nos referimos a las primeras publicaciones en español dentro del Proyecto Telecomunicaciones e Información de la UCM. Ver Corredoira, 1999 y 2001.

En España esto está ligado al Derecho Penal (Ribas, 2018) por la responsabilidad penal de las personas jurídicas exigible desde 2010; si bien hay ámbitos en los que se va extendiendo esta necesidad de que administradores, ejecutivos y empleados "cumplan" con determinadas normas éticas y jurídicas del sector.

Urge pues, conectar la transparencia a los derechos fundamentales para que esta no se vea como una cárcel, idea de panóptico de Benthan que retoma Han en su crítica a la sociedad de la transparencia.

Entre las políticas que España ha incorporado al mercado en esta línea –todavía sin una experiencia de años que permita valorarlo– es el sistema de compliance o cumplimiento de la legalidad, que la Comisión Nacional del Mercado y Competencia (CNMC) ha adoptado. Se trata de disposiciones para que las empresas "cumplan y hagan cumplir" la normativa sobre privacidad, datos, o incluso favorezcan buzones de denuncia. Son políticas de naturaleza privada para el sector económico, que fomenta la "transparencia" facilitando herramientas de cumplimiento para el contexto español (Nelson de Miranda, en Pérez Tremps, 2022: 292).

Apunto aquí esto que recoge el Parlamento Europeo con motivo de la comparecencia de Frances Haughen ya citada que dijo: "la UE tiene una oportunidad histórica de establecer estándares internacionales que inspiren a otros países". De hecho esta filtración de Facebook, junto con la reciente invasión y guerra de Ucrania ha precipitado que la UE se incline a un mayor control de contenidos en la red. Si acciones así van en la línea de pedir más rendición de cuentas, sí me encaja en nuestro sistema de valores, si no, no.

Afirma la web del Parlamento en esta línea mostrando la evolución en regulación, que se requiere más transparencia para poder elegir estando mejor y más informado.

En concreto el Parlamento Europeo (2017, nº 20 y 32) afirmaba que: "El Derecho debe dar respuestas en buena medida nuevas y precisamente la transparencia algorítmica y la rendición de cuentas son las vigas maestras de la garantías constitucionales frente a las decisiones algorítmicas". Veremos pronto cómo resultará el texto final de la Propuesta de Reglamento de IA.

Hay abundante bibliografía para aportar soluciones a los problemas de seguridad. Me refiero a la propuesta Libro Blanco Gobernanza de Internet sobre *Cyber-Atribución* (IGP White Paper, 2017)[13] donde se afirma que es complejo "atribuir de forma autorizada los ataques cibernéticos a los actores del Estado, y que dicha tarea requiere algo más que soluciones puramente técnicas". Entre otras soluciones, apunta la necesidad de "nuevas instituciones para mejorar la credibilidad, los controles y equilibrios procesales que pueden llevar la atribución más allá de una nación que señala con el dedo a uno de sus adversarios".

En concreto destacan –además, en la línea de lo que apuntábamos antes, que hacen falta peritajes e informes forenses que complementen las evidencias científicas e informativas–, que, si bien los gobiernos o sistemas de inteligencia atribuirán los ataques a intrusos específicos, "no existe un proceso forense reconocido internacionalmente con un nivel de confianza basado en pruebas. Y, sin un estándar reconocido y un proceso institucionalizado para la atribución, ¿podemos esperar que una coalición global implemente sanciones?"

Queda pues apuntado el cambio que hay que recorrer hacia un nuevo estándar en el ámbito de atribución, autoría de amenazas, de contenidos y por tanto de exigencias de responsabilidad.

Y, como fondo de todo el asunto que nos ocupa, *se trata de actualizar las garantías constitucionales, incluyendo los principios de los tribunales constitucionales* nacionales e internacionales, especialmente el Tribunal Europeo de Derechos Humanos y el Tribunal de Luxemburgo, para reconducir los ámbitos de falta de certidumbre y seguridad jurídica. En el ámbito de la transparencia y del acceso a la información es clave recuperar su relación con los principios democráticos. Como han destacado Troncoso, Villaverde o Ruiz-Rico en obra coordinada por Pérez Tremps (2021), el derecho a recibir como facultad del derecho a la información del art. 20 es el eje central, que debemos completar con el derecho a investigar, que si bien nuestra Constitución no

13 Traducción de la autora. El *Internet Governance Project White Paper* está disponible en https://via.hypothes.is/https://www.internetgovernance.org/wp-content/uploads/WhitePaper-Attribution-23-8.pdf (visitado el 30 de septiembre 2022).https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_ES.html

cita literalmente en el art. 20, si está como facultad del derecho del artículo 19 de la Declaración Universal de DDHH que el art. 10 reconoce como parte de nuestro texto constitucional.

VII. CONCLUSIONES

Concluyo sabiendo que hay mucho que estudiar y reflexionar aún.

Al problema anunciado en el primer apartado de este capítulo, dirigido a entender qué es de robots y qué de hombres en este mundo tecnologizado, sugiero que todo el ámbito del Derecho, legisladores, jueces y academia sigamos ponderando el impacto de las nuevas tecnologías en la forma de entender el derecho a la información y la libertad de expresión en la red, sin que nos arrolle la prisa y la dificultad de entender algunos parámetros. El objetivo es evitar la brecha entre el mundo real y el mundo de las normas legales.

En esta misma línea de entender mejor y legislar bien es preciso cualificar a legisladores y jueces para que en el ámbito público se evite la actuación o reacción en caliente. Se debe huir de regular tal o cual cuestión (como la suspensión de *Russia Today*, exigir el DNI en redes, por poner algunos ejemplos recientes) sólo por los peligros o males inminentes sin ponderar los daños que pueda afectar a bienes de mayor importancia (derechos, infancia, confianza en las instituciones, etc.).

Al problema segundo sobre la atribución, origen o autoría de bulos, ataques, o filtraciones, propongo afrontar el tratamiento "jurídico" de las noticias falsas, dentro de una amplia taxonomía de la desinformación, distinguiendo bien su origen y fin, y conociendo las recomendaciones internacionales, pero no poner en riesgo los derechos informativos. En este sentido las legislaciones sobre Facebook en Alemania, de redes en Francia o sobre campañas electorales en Italia[14], que se han visto enmendadas por los tribunales constitucionales, enseñan que debe actuarse con prudencia y ponderación de los derechos en juego. Nos referimos a la aplicación de la ley alemana *The Gesetz zur Verbesserung*

14 Caso relacionado con Casapound, por el Tribunal de Roma. La justicia italiana ordena a Facebook que reactive la cuenta de un partido neofascista, en prensa véase https://www.lavanguardia.com/internacional/20191213/472198574159/justicia-italiana-ordena-facebook-reactivar-cuenta-partido-neofascista.html (visitado el 30 de septiembre 2022).

der Rechtsdurchsetzung in sozialen Netzwerken ("NetzDG") de 1 de septiembre de 2017[15] o a la ley francesa Loi Nº 2020-766397 enmendada por el *Conseil constitutionnel français en la Décision* n° 2020-801 DC de 18 de junio de 2020[16].

En ese sentido, conviene unificar criterios internacionales en aspectos como la protección de datos o la protección de menores para evitar "paraísos" legales para la criminalidad telemática simplificaría el contexto, como ha ocurrido ya hace muchas décadas en el campo de la propiedad intelectual.

En el ámbito educativo, se requiere formación (alfabetización digital y algorítmica) ya no sólo ante los bulos, sino hacer planes de formación y alfabetización digital que partan de entender las redes en el contexto de la inteligencia artificial, en la línea del informe "Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil"[17] recientemente aprobado en España. También se requiere mucha pedagogía para la comprensión de nuevas realidades como el recién creado *Metaverso* en occidente, criticado aquí y allá por escapista y con su respuesta represiva en China (Pascual, 2022). En ese ámbito mostrar la distinción de mensajes y criterios (y herramientas) para la comprobación de fuentes (para el ciudadano) es crucial.

Al problema citado sobre las consecuencias que eso supone en el periodismo y en su credibilidad, como ya se ha dicho, los periodistas, la prensa, los medios informativos (no tanto la telerrealidad o el puro entretenimiento), debemos volver a los códigos de ética informativa y a acuerdos de auto-regulación serios con las grandes plataformas, también a una ética algorítmica (Salazar y Benjamins, 2022).

15 Disponible en inglés en https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html (visitado el 30 de septiembre 2022).

16 Disponible en https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm#:~:text=La%20diffusion%20d'images%20pornographiques,et%20aux%20droits%20des%20tiers (visitado el 30 de septiembre 2022).

17 Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil, de Presidencia del Gobierno de España (2022), iniciativa de cooperación público-privada impulsada por el Departamento de Seguridad Nacional (DSN). Disponible en https://www.dsn.gob.es/es/file/8031/download?token=gM-FWjCJ (visitado el 30 de septiembre 2022).

Desde los medios se han de actualizar los códigos éticos y las políticas o pautas de redacción teniendo en cuenta el papel de los algoritmos, y el alcance de la personalización masiva de información. La situación laboral actual de las empresas y medios ha dado por supuesta esa formación, y no parece suficiente.

Y finalmente, como profesionales del periodismo y como docentes del Derecho Constitucional, es fundamental recuperar la confianza en la objetividad y principios de la prensa libre que son la objetividad, el juego limpio, el rigor, la imparcialidad, la calidad y la honradez con uno mismo y con el público. Y esto, como pueden imaginarse, no se le puede pedir a un robot.

VIII. BIBLIOGRAFÍA

– ALANDETE, D. (2021): *Fake news: la nueva arma de destrucción masiva*, Zalla (Vizcaya), Deusto.

  - (2022): *Rusia o cómo usar las 'fake news' para convencer a su pueblo*, en el diario ABC, disponible en https://www.abc.es/tecnologia/redes/abci-rusia-o-como-usar-fake-news-para-convencer-pueblo-no-guerra-invasion-202203240115_noticia.html (visitado el 30 de septiembre 2022).

– Anónimo (2022): *Confesiones de un bot ruso*, Barcelona, Random House.

– ARELLANO, W. (2012) (Coord.): *La Sociedad de la Información en Iberoamérica. Estudio multidisciplinar*, Ciudad de México, INFOTEC.

– BEL MALLÉN, I. (2021): *La ética informativa: un reto en la era de la posverdad*, Valencia, Tirant lo blanc.

– CADWALLADR, C. (2017): "The great British Brexit robbery: how our democracy was hijacked", en *The Guardian*, 7-5-2017. Disponible en https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy (visitado el 30 de septiembre 2022).

– CETINA PRESUEL, R. y MARTINEZ SIERRA, J. M. (2019): "Algorithms and the News: Social Media Platforms as News Publishers and

Distributors". *Revista De Comunicación*, 18(2), pp. 261-285. Disponible en https://ssrn.com/abstract=3449188 (visitado el 30 de septiembre 2022).

– COMISIÓN EUROPEA (2017), *Fake News initiative*. Disponible en https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1184-Communication-on-fake-news-and-online-misinformation_es (visitado el 30 de septiembre 2022).

– CORREDOIRA, L. (1999): *Los retos jurídicos de la información en internet: Las libertades de acceso y difusión*, Universidad Complutense de Madrid, https://dialnet.unirioja.es/servlet/libro?codigo=1267

  - (2001), *La libertad de información, gobierno y arquitectura de Internet*, https://dialnet.unirioja.es/servlet/libro?codigo=460311 (visitado el 30 de septiembre 2022).

– CORREDOIRA, L. y COTINO, L. (2013) (eds.): *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Madrid, Centro de Estudios Políticos y Constitucionales (CEPC).

– COTINO, L. (2017), "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata* Núm. 24, Ética de datos, sociedad y ciudadanía, pp. 131-150. En https://www.dilemata.net/revista/index.php/dilemata/article/view/412000104 (visitado el 30 de septiembre 2022).

– GARCIA MEXÍA, P. (2009): *Derecho europeo de internet: hacia la autonomía académica y la globalidad geográfica*, Oleiros (La Coruña). Netbiblo.

– HAN, B. (2021): *Sociedad de la transparencia*, 1ª edición, Barcelona, Herder.

– IGP *Internet Governance Project White Paper*, 2017 https://via.hypothes.is/https://www.internetgovernance.org/wp-content/uploads/WhitePaper-Attribution-23-8.pdf (visitado el 30 de septiembre 2022).

– JUNCO, L. (2022): "De 'Mad Men' a 'Math Men': los nuevos perfiles publicitarios", en el diario *Expansión*, disponible en https://www.expansion.com/

directivos/2022/01/18/61e5aba3e5fdeafc268b460e.html(visitado el 30 de septiembre 2022).

– MANFREDI SÁNCHEZ, J. L., DEL FRESNO GARCIA, M. (2018): "Politics, hackers and partisan networking. Misinformation, national utility and free election in the Catalan independence movement", en *El profesional de la información*, Vol. 27, Nº 6, Ejemplar dedicado a: Información política y redes sociales (II), pp. 1225-1238.

– MORETÓN, A., (2012): *El secreto profesional de los periodistas: de deber ético a derecho fundamental*, Madrid, Centro de Estudios Políticos y Constitucionales.

- (2014): "La protección de las fuentes de información, la integración del modelo español con la jurisprudencia del TEDH", en *Estudios de Deusto: revista de Derecho Público*, Vol. 62, Nº. 2, 2014.

– PARLAMENTO EUROPEO, (2017): *Resolución de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley* (2016/2225(INI)), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_ES.html (visitado el 30 de septiembre 2022).

- (2020): *Informe sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación* (2020/2268(INI), Comisión Especial sobre Injerencias Extranjeras en todos los Procesos Democráticos de la Unión Europea, disponible en https://www.europarl.europa.eu/doceo/document/A-9-2022-0022_ES.html (visitado el 30 de septiembre 2022).

– PASCUAL, M. (2022): "Así es el metaverso que prepara China: alta tecnología para limitar la subversión. Pekín está organizando a la industria para desarrollar su versión de un entorno digital al que vincula con su seguridad nacional", en *El país* de 29.9.2022, disponible en https://elpais.com/tecnologia/2022-09-29/asi-es-el-metaverso-que-prepara-china-alta-tecnologia-para-limitar-la-subversion.html (visitado el 30 de septiembre 2022).

– PÉREZ-TREMPS, P., REVENGA SÁNCHEZ, M. (2021): *Transparencia, Acceso a la información pública y lucha contra la corrupción*, Valencia, Tirant lo blanc.

– PISANTY BARUCH, A. (2007): "Gobernanza de internet y los principios multistakeholder de la Cumbre Mundial de la Sociedad de la Información", en *Revista mexicana de política exterior,* 2006-2007, núm. 79-80, pp. 9-39.

– RIBAS, X. (2018): *Practicum Compliance*, Cizur (Navarra), Thomson Reuters.

– SALAZAR, I. y BENJAMINS, R. (2022): *Mi algoritmo y yo*, Madrid, Anaya.

– SNOWDEN, E. (2019): *Vigilancia permanente*, Barcelona, Planeta.

– WASSERMAN, E. (2017): "Safeguarding the News in the Era of Disruptive Sources", *Journal of Media Ethics, Exploring Questions of Media Morality*, Volume 32, 2017 - Issue 2, https://doi.org/10.1080/23736992.2017.1294020

– WYLIE, C. (2020): *Mindf*ck: Cambridge Analytica: la trama para desestabilizar el mundo*, Barcelona, Roca editorial.

– ZUBOFF, S. (2020): *La era del capitalismo de la vigilancia*, Madrid, Paidós.