Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad

Social Media, Disinformation, Cyber Sovereignty and Digital Surveillance: Vision from Cybersecurity

MARIANO CÉSAR BARTOLOMÉ

Colegio Interamericano de Defensa (Washington), Estados Unidos

RESUMEN: Luego de un desarrollo de cincuenta años, Internet es la piedra basal del ciberespacio. Los usuarios de esta red superan ampliamente la mitad de la población mundial y su influencia alcanza todos los aspectos de las sociedades contemporáneas. En la actualidad, la libertad de acceso a Internet está considerada dentro del campo de los Derechos Humanos; sin embargo, al mismo tiempo crecen las dudas acerca de la credibilidad de la información existente en la red, así como la preocupación por la privacidad de los datos personales que allí circulan. Este artículo se enfoca, desde una perspectiva de ciberseguridad, en tres aspectos vinculados al respeto de las garantías y derechos individuales: la accesibilidad a Internet y la vigilancia digital; el funcionamiento de las redes sociales y la privacidad de los datos personales que ellas emplean y almacenan; y el uso de las redes sociales en acciones de desinformación que incluyen noticias falsas (fake news) y narrativas de posverdad.

PALABRAS CLAVE: Ciberseguridad, Cibersoberanía, Desinformación, Redes Sociales, Vigilancia Digital.

ABSTRACT: After a development of more than fifty years, today the Internet has established itself as the key element of cyberspace. Network users exceed half of the world's population, while its impact reaches all sides of contemporary societies. Today, free access to the Internet is inserted in the field of human rights; however, at the same time, concerns about the credibility of information stored on the network are increasing. This article will focus, from the point of view of cybersecurity, on three main topics related to the respect of individual rights and guarantees: Internet accessibility and digital surveillance; social networks and the privacy of personal data; and the use of those social networks in the execution of disinformation operations that include fake news and post-truth narratives.

KEYWORDS: Cybersecurity, Cyber Sovereignty, Disinformation, Social Media, Digital Surveillance.

Recibido: 30 de julio de 2021. Aceptado: 13 de septiembre de 2021.

Revista de Estudios en Seguridad Internacional, Vol. 7, No. 2, (2021), pp. 167-185. http://www.seguridadinternacional.es/revista/

ISSN: 2444-6157. DOI: http://dx.doi.org/10.18847/1.14.9

INTRODUCCIÓN

Hace ya más de medio siglo, el 29 de octubre de 1969, desde la Universidad de California se envió un escueto mensaje al Instituto de Investigaciones de la Universidad de Stanford a través de una embrionaria red experimental de comunicaciones, cuyo desarrollo era financiado por el Departamento de Defensa. Así nació Internet, que poco más de cinco décadas después contaba como usuarios a más de 4,6 mil millones de personas, cifra que implica una tasa de penetración de casi el 60% de la población mundial (Kemp, 2021). Al mismo tiempo, los flujos de datos a través de esa red tuvieron un salto exponencial, pasando de 100 Gb diarios en 1992 a una previsión de 150,7 mil Gb por segundo para el año 2022 (UNCTAD, 2019). Una manera de graficar ese salto cuantitativo ha sido proporcionada por un asesor tecnológico de la Biblioteca del Congreso de Estados Unidos: si durante mucho tiempo esa institución fue considerada el mayor reservorio de información del planeta, en el año 2017 ya existía en Internet el equivalente a una colección de esa biblioteca cada siete personas. Las proyecciones, en ese momento, eran de alcanzar la proporción de una biblioteca por individuo, en apenas un lustro (Lissardy, 2017).

La idea de "macrodatos", más conocidos como *Big Data*, se vincula precisamente con esta nueva situación de los datos en circulación por Internet y puede ser comprendida como "un conjunto de herramientas informáticas y estadísticas que permiten simplificar, administrar, coordinar y analizar grandes volúmenes de información" (Monleón-Getino, 2015: 436). Las características de la información involucrada en el concepto Big Data suelen resumirse en la sigla 3V: tiene gran volumen, es extremadamente variada en su formato y circula a gran velocidad, prácticamente en tiempo real (Rey, 2020).

En lo que se conoce como "transformación digital", los productos y servicios asociados a este aumento de datos resultan disruptivos para numerosas actividades o prácticas tradicionales (UNCTAD, 2019). Entre esos servicios, ocupa un lugar especial la Inteligencia Artificial (IA), que refiere a sistemas capaces de examinar e interpretar grandes cantidades de datos para llevar a cabo tareas diversas, imitando en cierta forma el razonamiento humano. Dentro de la IA, el "aprendizaje automático" se ocupa del diseño y construcción de algoritmos que permiten a los ordenadores "aprender" por sí mismos, tomar decisiones o hacer predicciones, a partir de datos (UIT, 2020). En palabras de un especialista, esas actividades se llegan a realizar con la calidad digna de un experto (Monleón-Getino, 2015).

En definitiva, Internet es la piedra basal del ciberespacio, entendido de manera simplificada como un "entorno virtual de información e interacciones entre personas" (Kissinger, 2016). Este entorno está compuesto por redes, sistemas de información y telecomunicaciones (Quintana, 2016) y es considerado un "común global"; es decir, un dominio que no está bajo el control ni la jurisdicción de ningún Estado, pero su uso es materia de competencia por actores estatales y no estatales de todo el planeta (Stang, 2013). El impacto de Internet en las sociedades contemporáneas es enorme y ayuda a comprender por qué hoy el acceso a esta red está considerado dentro del campo de los Derechos Humanos. Esta percepción se observa con nitidez desde hace más de una década, según lo confirman diferentes sondeos de opinión.

En efecto, a inicios del pasado decenio una encuesta global llevada adelante por el servicio informativo británico BBC confirmó que cuatro de cada cinco adultos consideraban que el acceso a Internet era un derecho fundamental y que la red les había proporcionado una mayor

libertad, sobre todo de expresión. Un porcentaje aún más alto de encuestados (90%) afirmó que era un ámbito propicio para adquirir información y conocimientos (Reuters, 2010).[1] Con estos antecedentes, el Consejo de Derechos Humanos de la Asamblea General de la Organización de las Naciones Unidas (ONU) se manifestó en ese sentido y declaró el ingreso a Internet como un derecho humano (United Nations, 2011). De acuerdo al Relator Especial de la ONU sobre derecho a la libertad de opinión y expresión, Frank La Rue, autor del informe aprobado por ese órgano, la red "no sólo permite a los individuos ejercer su derecho de opinión y expresión, sino que también forma parte de sus derechos humanos y promueve el progreso de la sociedad en su conjunto" (Muñoz, 2011).

Desde aquellos momentos, en la visión de los usuarios de Internet, tendió a estabilizarse la vinculación de su acceso irrestricto con el respeto a las libertades y garantías individuales. Así, hace un lustro, el porcentaje de individuos que consideró a tal habilitación como un derecho humano básico alcanzó el 82% (GlobeScan, 2017). Sin embargo, en lo que *a priori* podría parecer un contrasentido, durante ese lapso alcanzaron similar intensidad las preocupaciones en torno a los efectos negativos que puede reportar un empleo intensivo de esa red. Al mismo tiempo que poco más de ocho cada diez internautas adherían al mencionado acceso irrestricto, se registraban tasas muy similares de dudas acerca de la credibilidad de la información existente en la red (79%) y de preocupación por la privacidad de los datos personales que allí circulan (80%) (GlobeScan, 2017; CIGI, 2019).

En el presente trabajo se abordarán desde una perspectiva de ciberseguridad tres aspectos vinculados al respeto de las garantías y derechos individuales: la accesibilidad a Internet y la vigilancia digital; el funcionamiento de las redes sociales y la privacidad de los datos personales; y el empleo de los factores precedentemente mencionados (Internet y redes sociales) para desinformar a los internautas con fines determinados.

Para alcanzar esa meta, el trabajo se estructura en la presente introducción, una fase desarrollo y unas breves conclusiones. El desarrollo se divide en tres partes, que se corresponden con igual cantidad de tópicos a analizar. Finalmente, en las conclusiones se incluirán contenidos de naturaleza prescriptiva. El análisis fluctuará entre los niveles descriptivo y explicativo, la información a emplear será predominantemente cualitativa y las fuentes serán secundarias.

Resta agregar que se entenderá a la ciberseguridad en los términos en que lo hace la Unión Internacional de Telecomunicaciones. Esa definición centra su foco en la protección de los activos y los usuarios (independientemente de su tipo) en el ciberespacio, con referencia a la disponibilidad, integridad y confidencialidad de la información. Textualmente:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno (UIT, 2010: 20).

[1] La encuesta fue realizada para la BBC por la empresa GlobeScan y el universo de análisis incluyó a 27 mil adultos en 26 países de todos los continentes.

LAS REDES SOCIALES Y LA PRIVACIDAD DE LOS DATOS PERSONALES

En los debates actuales en torno a la privacidad de los datos personales que fluyen por Internet, juegan un papel capital las llamadas "redes sociales", surgidas a lo largo de la primera década del siglo. Una definición simplificada de redes sociales es la que propone la Real Academia Española: "Plataforma digital de comunicación global que pone en contacto a gran número de usuarios" (IAB Spain, 2019: 14). La meta de ese contacto sería la creación de amistades y relaciones. Por eso, pueden ser entendidas como una reunión de individuos –conocidos o desconocidos- que interactúan entre sí, redefiniendo al grupo y retroalimentándolo (Caldevilla Domínguez, 2010). A los efectos de este trabajo, las entendemos como servicios basados en la *web* que permiten a los individuos construir un perfil público o semipúblico dentro de un sistema limitado; articular una lista de otros usuarios con quienes compartir una conexión; y combinar sus propias listas de conexiones con aquellas elaboradas por otros dentro del sistema (Boyd & Ellison 2007). En el período comprendido entre los años 2004 y 2010, surgieron los cinco servicios más conocidos y difundidos en esta materia: Facebook, Youtube, Whatsapp, Instagram y Twitter.

Con ese marco, a través de las redes sociales sus usuarios llevan adelante diferentes actividades, incluso a escala planetaria. Entre otras, envían mensajes públicos o privados; compran o venden productos y servicios (*e-commerce*); adquieren destrezas y conocimientos, sobre diferentes temas; buscan u ofrecen empleo; siguen de manera periódica personas o marcas; se mantienen actualizados en determinados rubros; comparten contenidos propios, y conocen gente.

Las últimas estadísticas disponibles (Chaffey, 2021) confirman la expansión de las redes sociales: hoy alcanzan a 4,2 mil millones de personas, o el 53,6% de la población mundial, con un crecimiento interanual del 13%, equivalente a un agregado de 490 millones de individuos. Del total de personas conectadas a las redes, casi el 99% (4,15 mil millones) lo hace a través de dispositivos móviles (telefonía celular). Una interesante perspectiva sobre la dimensión de estas redes propone pensar a sus usuarios como ciudadanos de países; desde este punto de vista, Facebook y Youtube tendrían "más población" que China o la India, que quedarían relegados al tercer y cuarto puesto, respectivamente. Tras estas dos naciones asiáticas se enlistan al menos otras ocho plataformas de ese tipo, apareciendo Estados Unidos recién en el decimotercer lugar (Jaimovich, 2019).[2]

Las redes sociales no sólo congregan en torno suyo a miles de millones de internautas, sino que suelen ser consultadas con una frecuencia diaria, e incluso -según el caso- numerosas veces al día, totalizando varias horas. No sería errado sostener que configuran una suerte de adicción, generando en el usuario un placer que se puede corroborar clínicamente, a partir del neurotransmisor denominado *dopamina*. Aunque existe consenso entre los especialistas en torno a los dilatados lapsos de conexión a las redes sociales, la información de respaldo disponible es escasa y fragmentaria. No obstante, el caso de España proporciona interesantes datos en este sentido, susceptibles de ser aplicados en el análisis de otros países. Allí, las diez redes sociales con mayor penetración en el mercado local son visitadas diariamente por al

[2] En este artículo se calculaba a los usuarios de Facebook y Youtube en 2300 y 1900 millones de personas, respectivamente. Los últimos guarismos elevan sendos totales a 2740 y casi 2300 millones, ampliándose así la diferencia con China y la India. Además, entre *youtubers* y chinos deberían ubicarse a los usuarios de Whatsapp, no computados en el artículo periodístico y estimados en 2000 millones de personas (Chaffey, 2021).

menos la mitad de sus usuarios. Enfocando la atención solamente en las tres primeras redes de ese ranking, cada día acceden a Whatsapp el 97% de sus clientes, a Facebook el 74% y a Instagram el 71%; en el primero de estos casos, el 85% de los visitantes lo hace varias veces por día, tasa que es de casi el 50% en los otros dos (IAB Spain, 2019).

Resulta conveniente incorporar, en este punto del análisis, una breve referencia a Google, una empresa del grupo Alphabet, propietaria también de Youtube. Técnicamente no es una red social, sino un conjunto de servicios estructurados en torno a su motor de búsqueda, consolidado como el más empleado a nivel mundial. A través de esos servicios, recoge gran cantidad de información sobre sus usuarios, elaborando perfiles sobre su conducta e intereses. En los términos de un conocido periodista científico estadounidense, un internauta puede llegar a dedicar más de siete horas diarias a los productos relacionados con Google, agregando:

> La compañía de Silicon Valley ha aprovechado el acto de buscar algo on-line en un **i**mperio tecnológico tan grande que se ha colado en mi casa, mi trabajo, mis dispositivos y mucho más (…) se ha convertido en la marca de tecnología que domina mi vida (Chen, 2020).

Como se anticipó en párrafos previos, pese a sus altas tasas de penetración y de frecuencia de uso, o precisamente debido a ese motivo, las redes sociales concentran las mayores preocupaciones en lo que hace a la naturaleza privada de los datos personales en Internet. La cuestión se vincula con la importante cantidad de información de sus usuarios que tienen las redes, y las incógnitas que se plantean en torno a su preservación y empleo. Cobo (2019) indica que la privacidad de los datos, en los espacios digitales, se ha tornado en un bien escaso al cual prácticamente no puede acceder el ciudadano normal. La única manera de lograrla sería produciendo una desconexión con todos los canales digitales y servicios asociados, una opción que por su alto costo suele descartarse. Karanicolas (2014) nos dice que, al ponerse en riesgo la privacidad de sus datos personales, los usuarios de Internet ven comprometido su anonimato, un valor particularmente importante en el plano cibernético, desde el momento en que proporciona una sensación de libertad. Libertad para seguir gustos e intereses secretos, o para expresar opiniones o sentimientos, sin miedos. El anonimato también opera como protección frente a diferentes contingencias, desde la vergüenza a la violencia real.

En este sentido, una reciente investigación a escala global indica que Facebook e Instagram son quienes almacenan la mayor cantidad de datos personales de sus usuarios, con la plataforma de citas Tinder en tercer lugar (Conversia, 2020).[3] Cabe aclarar que el cálculo se realiza en base al total de información personal que el usuario autoriza a la red social a recabar, al momento de comenzar a emplearla, a través de la firma de extensos acuerdos de términos y condiciones. Sin embargo, debido a su longitud y al complejo vocabulario que emplean, esos requisitos raramente se leen, razón por la cual los internautas desconocen el permiso que están otorgando (LePan, 2020).[4] Por otro lado, un estudio realizado en la

[3] El estudio en cuestión fue realizado por la compañía de seguridad informática Clario Tech. La información que recopilan las redes sociales incluye nombre, profesión o actividad laboral, salario, edad, fecha y lugar de nacimiento, lugar de residencia, medidas corporales, orientación sexual, creencias religiosas, hobbies o pasatiempos y gustos musicales, entre otros. Con este contexto, Facebook almacena el 70% de los datos personales que el usuario le habilita a recolectar, Instagram el 59% y Tinder el 53%.

[4] Estos resultados se desprenden de un estudio realizado por la consultora Visual Capitalist tomando como universo de análisis a veintiuna redes sociales, aplicaciones y plataformas digitales. El tiempo de lectura se calculó en idioma inglés, a partir de la extensión de los acuerdos de términos y condiciones de uso de estas

Universidad de Oxford indicó que las redes sociales también reciben información direccionada desde la mayoría de las aplicaciones (entendidas como un tipo de software diseñado para ser ejecutado en dispositivos móviles, que permite al usuario realizar uno o más tipos de trabajo específicos). Según ese relevamiento, el 88% de los datos fluyen a Alphabet (Google, Youtube), 42% a Facebook (incluye a Instagram y Whatsapp) y 33% a Twitter (Payo, 2018).

La razón que subyace a tal almacenamiento consiste, esencialmente, en mostrar al usuario anuncios publicitarios personalizados que pueden ser de su interés, instando a su consumo. Así, los datos personales adquieren un enorme valor y se transforman en un bien altamente codiciado y demandado en Internet, que se transforma *de facto* en un gran mecanismo para su recolección (Karanicolas, 2014). En este sentido, Hilbert se remite a investigaciones de la Universidad de Cambridge, realizadas sobre una muestra representativa de usuarios habituales de Facebook, para señalar que un centenar de "clicks" le permiten a los algoritmos de esa red social detectar aspectos relevantes del perfil del individuo en cuestión: orientación sexual, identidad étnica y religiosa, postura política, nivel de inteligencia, incluso vicios y pasatiempos (Lissardy, 2017). Otras fuentes coinciden en la capacidad predictiva de los algoritmos de Facebook, asegurando que con una decena de clicks pueden superar en este campo a los colegas de trabajo de la persona en cuestión; con setenta, a sus amigos; con ciento cincuenta a sus familiares, e incluso a sus cónyuges, con trescientos (Sampedro Oliver, 2021).

Esta cuestión crucial ha sido tratada en profundidad a través de diversos trabajos recientes (Cobo, 2019; Peirano, 2019; Zuboff, 2020), destacando que los sistemas digitales que se usan de forma gratuita en realidad cobran su uso por medio del acceso a los mencionados datos. A su vez, a través del mencionado "aprendizaje automático", ese material alimenta a un conjunto de algoritmos que nos devuelve publicidad e información. Así, esos sistemas influyen en la realidad del usuario, en su forma de pensar y actuar. Como sugiere el fenómeno conocido como "burbuja filtro" (*filter bubble*), esa influencia incluye la presentación al consumidor de contenidos cada vez más personalizados a sus gustos, reduciéndose las visiones o lecturas divergentes (Garro, 2016). Debido al denominado "sesgo de confirmación", esos contenidos serán aceptados por el individuo, precisamente por ser compatibles con sus propios gustos, creencias y posiciones.

Los conceptos "capitalismo de vigilancia" y "economía de la atención"[5] caminan en el sentido de las apreciaciones precedentes y son complementarios entre sí. Por medio del primero de ellos, Zuboff (2020) señala que algunas empresas del mundo digital consideran a la experiencia humana privada como una materia prima que se puede traducir en datos. Esa experiencia es procesada y "vendida" como producto de predicción de la conducta de su protagonista, que de esa manera pierde el control sobre tales datos personales. En los términos de esta profesora emérita de la Universidad de Harvard, la gente común deviene en

compañías, medida en palabras, tomando como referencia que una persona adulta y educada lee un promedio de 240 palabras por minuto. La pesquisa indicó, además, que el 97% de los usuarios de redes sociales, aplicaciones y plataformas suele aceptar sus términos de uso sin haber realizado una lectura de las condiciones.

[5] Este concepto corresponde al economista Herbert Simon, Premio Nobel de Economía, e indica que lo que la información consume es bastante obvio: la atención de sus consumidores. Por lo tanto, una gran cantidad de información crea una pobreza de atención y la necesidad de asignar esa atención eficientemente entre la abundancia de fuentes de información que podrían consumirla.

títere de un puñado de titiriteros tecnológicos que moldean su comportamiento (Zuboff, 2020). Y lo hacen al extremo de poner en duda la idea de la libertad de las acciones del individuo, siendo que tal vez lo que realmente hay es ignorancia sobre los elementos que condicionan sus decisiones (Magnani, 2020). Por su parte, la economía de la atención ocupa un lugar central en el planteo de Peirano (2019), según el cual la dinámica de Internet consiste, en buena medida, en captar la limitada capacidad de atención de los usuarios, para luego influir en su impulso consumista y así poder vender sus productos. Desde esta perspectiva, cuanto mayor sea la cantidad de información sobre los usuarios que puedan obtener las *apps* y redes sociales, de mejor manera podrán captar su atención y más dinero harán ganar a las compañías.

A modo de corolario, los enfoques de Zuboff y Cobo desde la academia, y de Peirano desde el periodismo independiente, se confirman en el campo cinematográfico con el reciente documental El Dilema de las Redes Sociales (*The Social Dilemma*), dirigido por Jeff Orlovski.[6] Su línea argumental plantea, precisamente, que las redes sociales están diseñadas para captar la atención de los individuos y que pasen más tiempo en ellas; que ese tiempo es lo que las redes venden; y que lo que monetiza a esos sitios es su capacidad de atraer y retener individuos. Accesoriamente, a través de la información que les proveen, las redes sociales son capaces de interferir en los comportamientos reales de sus usuarios, afectando su forma de actuar y cómo se sienten. En otras palabras, los manipulan, o están en condiciones de hacerlo.

La desinformación en Internet

Ya se indicó que, junto a la privacidad de los datos personales, la credibilidad de la información existente en Internet es motivo de gran preocupación. En este punto, tres conceptos centrales parecen dominar el escenario: noticias falsas (cuestión más conocida por su versión en inglés, *fake news*, que emplearemos en adelante), posverdad y desinformación. Yendo al primero de ellos, Ford (2020, 2021) explica que se refiere a noticias que, a pesar de no ser ciertas, se comparten deliberadamente para hacer daño con un objetivo establecido. *In extenso*, esas noticias tienen el propósito de difundir información que no es real, pero es verosímil y creíble, a los efectos de manipular las acciones y el pensamiento de los individuos, y así crear una atmósfera de temor y pánico que bloquee el raciocinio y el juicio crítico. Una atmósfera que, en la visión de esta especialista, puede llegar a desestabilizar un gobierno y arriesgar la vigencia de la democracia. Las noticias falsas (o falsedades profundas), *deep fakes* en inglés, constituyen un subtipo de las primeras que incluso profundiza y agrava sus efectos. Aunque existen desde fines del siglo pasado, alcanzaron alta notoriedad durante el último decenio. Constituyen archivos de video, imagen o voz con apariencia realista, manipulados mediante Inteligencia Artificial, en los cuales personas dicen o hacen cosas que en realidad no dijeron ni hicieron (Toews, 2020).

Los riesgos de las *deep fakes* son múltiples e imposibles de soslayar. Alcanzan los planos político, social, económico y también internacional. Un informe de *Brookings* destaca entre esos peligros a la distorsión del discurso democrático; la manipulación de elecciones; la erosión de la confianza ciudadana en las instituciones; el debilitamiento del periodismo; la

[6] Una presentación de este documental se puede consultar en la red Youtube: https://www.youtube.com/watch?v=QEiRXsEqpCA&feature=emb_logo

exacerbación de divisiones sociales; el deterioro de la seguridad pública, y el daño a la reputación de personalidades relevantes (Galston, 2020). En estos términos, no es exagerada la apreciación de Chesney y Citron (2018) cuando señalan que, en términos sistémicos, la afectación es al normal funcionamiento de la democracia. Específicamente en la esfera de las relaciones internacionales, el análisis de una crisis protagonizada por Qatar y Emiratos Árabes Unidos (Riordan, 2019) confirmó que las *deep fakes* pueden generar conflictos, o reactivar tensiones larvadas o latentes, que incluso podrían escalar al empleo de la fuerza.

Las *fake news* pueden adoptar diferentes formatos, dando lugar a distintas tipologías. A los efectos del presente trabajo, identificamos las siguientes formas principales, que pueden presentarse en forma independiente o combinadas entre sí: información inventada, cuando su contenido es completamente falso; información manipulada, a partir del tratamiento de datos o imágenes reales; información de fuentes falsas, en las cuales se observa la creación y difusión de contenidos suplantando fuentes oficiales; contenidos verdaderos combinados con un contexto falso; contenidos que tienen una conexión falsa con el título, con el cual no guardan relación; finalmente, sátiras y parodias, es decir, informaciones humorísticas que se presentan como si fueran ciertas, pudiendo engañar a los lectores de forma no intencionada (Morales, 2019; Rojas Caja, 2020).

Las noticias falsas encuentran su mejor caja de resonancia en las redes sociales, que han desplazado a los medios de comunicación como principales fuentes de información para amplios sectores de las sociedades contemporáneas. Esto es especialmente nítido en los sectores etarios más jóvenes, que no convivieron con los medios periodísticos impresos ni consumen la televisión tradicional, optando por alternativas que les permiten "estar al día" con los contenidos que ellos mismos seleccionan, aun cuando su calidad sea cuestionable (Marcos, Sánchez y Olivera, 2017; Sampedro, 2021). La dimensión que adquirió la cuestión se constata al comprobar que, según sondeos de alcance global, el 67% de los usuarios de Internet habría comprobado la presencia de noticias falsas en Facebook, el 65% en otras redes sociales, e incluso ocho de cada diez internautas aseguran haber sido víctima de ese tipo de contenidos al menos una vez (CIGI, 2019). Estas tasas podrían ser incluso más altas, si se tiene en cuenta que más del 60% de la población mundial no se siente capaz de distinguir entre noticias verídicas y rumores (Morales, 2019). En conjunto, esta situación resulta funcional a la expansión de la posverdad, entendida como "la tendencia por la que los hechos objetivos son menos influyentes en la opinión pública que las emociones y creencias personales" (Morales, 2019).

En esta línea, la verdad pierde algo de relevancia o importancia, pues compite con "otras verdades" alternativas que pujan por la preferencia del consumidor. En ese sentido, no puede negarse la existencia de cierto menosprecio de los hechos concretos, la razón y la evidencia verificable, resultando en una distorsión de la realidad. No obstante, estas lecturas alternativas suelen gozar de aceptación entre individuos que registran afinidad con ellas (Lozano, 2020; Marcos, Sánchez y Olivera, 2017). Posverdad y *fake news*, a la postre, constituyen la esencia de las acciones de desinformación, en el sentido de

> Aquella información que es verificablemente falsa o engañosa y que se crea, presenta y difunde para obtener beneficios económicos o para engañar intencionadamente al público, distorsionar el debate público, socavar la confianza de los ciudadanos e incluso desestabilizar los procesos democráticos (Rojas Caja, 2020: 4).

Las acciones de desinformación son el resultado de complejos procesos que abarcan el análisis del "blanco" de la iniciativa, incluyendo sus preferencias y vulnerabilidades, la creación de narrativas *ad-hoc* y la selección de los canales que se utilizarán en su ejecución. Su empleo se encuentra favorecido por importantes dificultades existentes, en materia de atribución de responsabilidad, y el abanico de los canales posibles abarca desde conocidas redes sociales, a medios propios preexistentes, o creados a tal efecto (CCN-CERT, 2019).

La inquietud que generan estas iniciativas, a nivel global, no es desdeñable: siete de cada diez personas están preocupadas por el eventual empleo de información falsa en Internet, de manera voluntaria, a modo de arma (Edelman, 2018). Y en modo alguno esta preocupación es infundada, si se tiene en cuenta que desde al menos una década se conforman equipos gubernamentales civiles o militares, de partidos políticos, la sociedad civil y el ámbito privado, ocupados en la manipulación de la opinión pública a través de las redes sociales. En el caso de gobiernos democráticos, las acciones oficiales apuntan más allá de las fronteras nacionales, en tanto los partidos políticos enfatizan en la esfera doméstica. Por el contrario, regímenes autoritarios o totalitarios enfatizan en el plano interno y sólo secundariamente en el externo (Bradshaw & Howard, 2017).

En la perspectiva de Estados Unidos y sus aliados de la Organización del Tratado del Atlántico Norte (OTAN), Rusia lleva adelante un constante e intensivo empleo de operaciones de desinformación. En esta lógica deberían entenderse las acciones desplegadas en torno a las elecciones presidenciales estadounidenses del año 2016, diseñadas y ejecutadas en buena medida desde la Agencia de Investigación de Internet (IRA). Esta institución está ubicada en San Petersburgo y, pese a su posición presuntamente independiente, operó según lineamientos del Poder Ejecutivo de ese país (Mac Farquhar, 2018; Sampedro, 2021). La injerencia en el proceso electoral consistió en el diseño y difusión de miles de anuncios políticos a través de centenares de cuentas falsas sobre todo en Facebook, subsidiariamente en Twitter e Instagram, además del uso de la plataforma Google (Redondo, 2017; CCN-CERT, 2019). Los dos informes elaborados por el Congreso de Estados Unidos país como resultado de las pesquisas llevadas adelante por su Comisión de Inteligencia indicaron que una veintena de páginas de Facebook manejadas por IRA fueron visitadas por 126 millones de personas y sus contenidos obtuvieron 39 millones de "clicks" de aprobación ("me gusta"); otros 20 millones de personas visitaron las páginas de Instagram regenteadas por la Agencia (Timberg & Romm, 2018).

Más cerca en el tiempo, la pandemia Covid-19 sirvió de marco para la ejecución de operaciones de desinformación de diferente tipo, por parte de una gran variedad de actores. Estas acciones tuvieron una intensidad tal, que la Organización Mundial de la Salud (OMS) se refirió a ellas en su conjunto a través de un neologismo, *infodemia*, entendida como "una sobreabundancia de información, algunas veces precisa, otras no, que dificulta que las personas encuentren fuentes fidedignas y orientación confiable cuando la necesitan" (Ford, 2020:57; OMS, 2020). De acuerdo con la lectura de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2020), su gravedad suele potenciarse en la medida en que incluye elementos emocionales, o es transmitida por comunicadores influyentes. Por otra parte, muchas veces incorpora importantes contenidos xenófobos o racistas. Este estado de cosas ha redundado en una creciente polarización entre la ciudadanía y los gobiernos, una reducción de la confianza de la primera en los segundos, y eventualmente en cuadros de desestabilización política y pérdida de cohesión social. Accesoriamente, esas

sociedades ven mermadas su capacidad de resiliencia frente a la pandemia (Hoogensen Gjørv, 2020).

El acceso a Internet: vigilancia digital y ciberSoberanía

Además de la privacidad de los datos personales y la difusión de falsa información en Internet, desde la perspectiva de la ciberseguridad interesa también la cuestión de la libertad con que acceden a las redes sociales y plataformas digitales los interesados en emplearlas. Un interrogante asociado al anterior es hasta qué punto los gobiernos no ejercen a través de ellas tareas de observación y supervisión de sus ciudadanos. Así, nos adentramos en el campo de la llamada "vigilancia digital", que básicamente se refiere al despliegue en el dominio digital de actividades de vigilancia. A los efectos del presente trabajo, se la entiende como "la observación de informaciones personales de forma intencional, rutinaria y sistemática con fines de control, derecho y legitimidad, gestión, influencia o protección" (Monnerat Lot & Barros Cianconi, 2018: 120). Aunque esta actividad dista de ser nueva, sus formas y métodos se han adaptado a las nuevas posibilidades tecnológicas, empleando el Big Data y la Inteligencia Artificial para identificar y reconocer patrones de comportamiento, de forma automática y masiva.

Durante todo el presente siglo, numerosos regímenes han justificado el uso y despliegue de tecnologías de vigilancia digital en la lucha contra amenazas transnacionales, tales como el terrorismo o el crimen organizado. Sin embargo, de esa forma se ejerce un control indiscriminado sobre el comportamiento de los ciudadanos, llegando en algunas situaciones a menoscabar sus derechos y libertades, al resultar intrusivas respecto a la protección de la vida íntima y de los datos personales (Santiago y Rodríguez, 2018). Los ciudadanos que se encuentren bajo vigilancia no suelen estar informados de estas prácticas, ni tienen acceso a los registros donde se recogen sus datos privados. Por otro lado, las autoridades encargadas de las actividades de vigilancia no suelen reconocer abusos o errores, ni se hacen responsables de los mismos.

Desde el punto de vista jurídico, la vigilancia digital contraviene una numerosa normativa internacional. Respecto a la Declaración Universal de Derechos Humanos de 1948, se destacan el artículo 12, según el cual nadie puede ser objeto de injerencias arbitrarias en su vida privada, y el artículo 19 que reafirma el derecho de todo individuo a la libertad de opinión y de expresión. También cabe mencionar la Convención Internacional de Derechos Civiles y Políticos de 1966, cuyo artículo 17 indica que nadie puede ser sujeto de interferencia arbitraria o ilegal a su privacidad, familia, hogar o correspondencia. A esto se agregan los así llamados "derechos ARCO" (acceso, rectificación, cancelación y oposición) relativos a la información personal, cuyo desarrollo excede los objetivos del presente trabajo.

Históricamente, la vigilancia digital ha estado asociada a regímenes políticos de características autoritarias, o incluso totalitarias, que aplican esa conducta sobre su propia población, con cierta periodicidad e incluso en forma permanente. Por eso, parece acertado aplicar a esos regímenes el apelativo de "autoritarismo digital" (Rozpedowski, 2021). Como ha indicado un especialista, "en un Estado vigilante se parte del supuesto que todos somos culpables" (Hypponen, 2014: 120). Rusia, y particularmente China, suelen ser los casos paradigmáticos en este sentido. En este último país, el Partido Comunista ejerce un escrutinio y control permanente de la actividad cibernética de la población, haciendo extensivo a este

campo el alcance del sistema de premios y castigos conocido como "créditos sociales". Este sistema ha sido calificado como "orwelliano" (Rathi, 2020) y se basa en la manipulación del puntaje personal de un ciudadano, según su comportamiento social. Por ejemplo, los créditos impactan en la autorización a viajar dentro del país o fuera de él, o en el acceso a servicios básicos (Rozpedowski, 2021; Sampedro, 2021).

La vigilancia digital china incluye la censura, ejercida desde organismos oficiales o promovida desde el Estado para que sea practicada voluntariamente por las mismas empresas y entidades de la sociedad civil, a modo de autocontrol. Para eso, estos actores suelen incorporar a su plantilla a especialistas que revisan sus contenidos *on line*, o contratan para estos menesteres a firmas dedicadas a la revisión de contenidos, reconocidas por el gobierno (Yuan, 2019).

Este tipo de prácticas ha sido explicado a partir de una concepción alternativa de la ciberseguridad, a la prevaleciente en Occidente. Esta diferencia de enfoque ayuda a comprender la razón por la cual hasta el momento no pudo plasmarse en las Naciones Unidas una convención amplia sobre la cuestión, que abarque sus aristas más importantes y goce de un alto grado de consenso (Anguita y Bartolomé, 2021). Ahondando sobre la cuestión, como se anticipó al inicio de este texto, en el Oeste ese concepto suele referirse a la protección de los activos y los usuarios en el ciberespacio, y la accesibilidad, integridad y confidencialidad de la información.

En casos como el chino o el ruso, en cambio, la ciberseguridad también alcanza a los contenidos, que pueden ser considerados una amenaza en sí misma. Un repaso sobre estos dos casos (Gady & Austin, 2010; Gold, 2019; Urgessa, 2020) confirma que, desde las postrimerías del siglo pasado, Rusia sostiene la postura de "información como amenaza" y consecuentemente implementó diferentes medidas de mantenimiento de control sobre ese activo. En cuanto a la visión oficial de China, ésta justifica prácticas de vigilancia en la necesidad de prevenir la infiltración ideológica y la instigación política. El eje de la cuestión se traslada así a la información, comprendida como un arma en sí misma, que puede ser enviada a través del ciberespacio (Tsaruk & Korniiets, 2020).

La "cibersoberanía" es una herramienta clave para el ejercicio de la vigilancia digital. Puede ser entendida como una acción a través de la cual "cada gobierno impone sus propias regulaciones de Internet, en una forma que restringe el flujo de información a través de las fronteras nacionales" (Freedom House, 2020: 2). Las razones que suelen esgrimirse para justificar estas restricciones son diversas, aunque usualmente se argumenta que son necesarias para hacer frente a crecientes amenazas internas y externas. Más específicamente, se invoca la defensa de la autoridad del gobierno, la moderación de la disidencia pública, la lucha contra el terrorismo, la preservación de la seguridad nacional y la protección del comercio y los intereses económicos locales (UNESCO, 2018). Estas limitaciones varían en forma e intensidad, siendo su expresión extrema el bloqueo absoluto al acceso a Internet. Apelando a la escala de "ciberpoder" de Nye (2010), esta opción suele ser interpretada como una suerte de manifestación de "poder duro", dando lugar a intensas críticas externas que llevan a dudar sobre la conveniencia de su aplicación (Jaitner, 2013).

Investigaciones independientes (Freedom House, 2020) indican que apenas el 20% de los usuarios mundiales de Internet accede a esa red en forma totalmente libre e irrestricta. Para el 35% de los internautas del planeta, ese acceso está fuertemente controlado y condicionado,

en tanto para otro 32% lo es sólo parcialmente (sobre el 13% remanente no se dispone de datos confiables). Siempre de acuerdo a esa fuente, el 73% de los usuarios de Internet de todo el orbe vive en países donde se producen detenciones y arrestos justificados en información política, social o religiosa subida a esa red. Además, el 64% de esos individuos habita países donde esas acciones han generado ataques físicos directos contra sus autores, e incluso asesinatos. Y el 56% lo hace bajo regímenes políticos cuyo aparato estatal periódicamente bloquea el acceso a determinados contenidos *on-line*.

En tiempos recientes, un elocuente y reciente ejemplo de cibersoberanía fue el caso que tuvo como protagonista a la marca occidental de indumentaria H&M. En el año 2020, esta cadena anunció que dejaría de adquirir algodón procedente de la región noroccidental china de Xinjiang, hasta tanto se aclararan las acusaciones de empleo de mano de obra esclava de la etnia local *uigur* en esa actividad textil. Tras un airado rechazo a esas sospechas por parte del Comité Central del PCCH, que de manera velada anticipó inminentes represalias, H&M fue virtualmente eliminado de todas las redes sociales chinas: sus tiendas dejaron de aparecer en los buscadores y en las plataformas de compras on-line, e incluso en las redes de *delivery* de comidas o de renta de automóviles. Esta dura respuesta habría disuadido a otras cadenas occidentales de indumentaria, que también emplean algodón de Xinjiang (entre ellas las gigantes Adidas y Nike), de adoptar posturas críticas similares a las de H&M (Merino, 2021).

En la actual coyuntura sanitaria internacional, los debates sobre vigilancia digital y los derechos de la población se encuentran atravesados por la pandemia de COVID-19. La UNESCO (2020) ha calificado a este acontecimiento como una crisis con claro impacto negativo en la libertad de expresión, el acceso a la información y la privacidad, aceptando ciertas restricciones temporales, fundamentadas en la salud pública. Sin embargo, el organismo también ha alertado sobre las aplicaciones desproporcionadas de estas medidas, sin un marco jurídico adecuado, o necesidad imperiosa, o con existencia de dudas sobre la legitimidad del propósito esgrimido por las autoridades gubernamentales.

Precisamente, en China y otras naciones del Extremo Oriente, incluso democracias consolidadas como Japón y Corea del Sur, los gobiernos han echado mano a sistemas de vigilancia digital, basados en el manejo de Big Data, para enfrentar a la pandemia. Estos mecanismos podrían ser considerados lesivos a la privacidad y a las libertades de expresión y asociación, pues registran y supervisan cada movimiento de los ciudadanos, evaluando su impacto en la crisis sanitaria. En consecuencia, se facilita el proceso de toma de decisiones, y en ese sentido el filósofo surcoreano Byung-Chul Han ha dicho: “Se podría decir que, en Asia, a las epidemias no las combaten sólo los virólogos y epidemiólogos, sino sobre todo también los informáticos y los especialistas en macrodatos” (Malaspina, 2020).

Las prácticas de vigilancia digital y cibersoberanía son motivo de seria preocupación para las Naciones Unidas. Esta institución intenta articular iniciativas de gobernanza en esta materia, apuntando a la libertad de acceso a Internet y el respeto a la privacidad de los datos personales que allí fluyen. Un trabajo reciente (Anguita y Bartolomé, 2021) señala que el monitoreo de la evolución de estas cuestiones a nivel global corre por cuenta de la Oficina del Alto Comisionado de los Derechos Humanos, aunque también desempeñan importantes roles otros órganos de ese sistema, destacándose la UNESCO y la Conferencia de las Naciones Unidas para el Comercio y el Desarrollo (UNCTAD).

La agencia con sede en París se enfoca en la universalidad del acceso a Internet a nivel nacional, evaluándola cualitativamente de acuerdo a cuatro principios fundamentales, que resumen su posición en este campo: una red abierta, accesible para todos los interesados, basada en derechos cumplidos en forma estricta y gobernada a través de la cooperación de múltiples partes interesadas. Esta visión se plasma en el "marco DAAM", acrónimo conformado por las siglas de los principios mencionados (Souter y Van der Spuy, 2018).[7] La Conferencia, por su parte, analiza la cuestión de la privacidad y protección de datos en el ciberespacio, en el marco de un registro actualizado de la legislación existente en relación a ese dominio, en todos los Estados miembros. De acuerdo a las últimas actualizaciones del "Seguidor Global de Ciberleyes" montado con ese objetivo (UNCTAD, s/f), actualmente existe legislación sobre protección de datos personales y privacidad en el ciberespacio en el 96% de los países de Europa, 69% de América, 57% de Asia y 50% de África. Desde otra perspectiva, cuentan con leyes de ese tipo el 89% de las naciones desarrolladas, 63% en vías de desarrollo y 43% de bajo desarrollo.

CONCLUSIONES

El crecimiento sostenido de Internet, desde sus primeros pasos hace más de medio siglo, junto a la expansión y consolidación del ciberespacio, constituyen eventos que han tenido un enorme impacto en todos los aspectos del funcionamiento de las sociedades contemporáneas. Un impacto que se incrementará en forma sostenida a corto y mediano plazo, según lo anticipan los desarrollos tecnológicos en curso y algunos conceptos que comienzan a integrarse a nuestro léxico cotidiano. A modo de ejemplos, se pueden citar la Cuarta Revolución Industrial, el Internet de las Cosas (IoT) y las redes 5G.

La ciberseguridad, enfocada en las amenazas y riesgos que se presentan y despliegan en el ciberespacio, incluye dentro de su esfera de interés todo lo relativo al enorme volumen de datos que fluye a través de Internet y que se plasma en el concepto Big Data. En forma más específica, como lo indica su conceptualización, atiende a la disponibilidad, integridad y confidencialidad de esa información. De esa manera, son cuestiones de su competencia la libertad de acceso a Internet, considerado un derecho humano básico; la credibilidad de la información existente en la red, en vistas a su eventual manipulación; y el manejo de los datos personales que circulan por ella, desde la perspectiva del derecho a la privacidad. En la actualidad, estos tres temas generan severas preocupaciones entre los internautas que, lejos de ser infundadas, gozan de importante sustento.

Las redes sociales, que hoy alcanzan a más de la mitad de la población mundial, juegan un rol central en los debates en torno a la privacidad de los datos personales. Esta importancia se fundamenta en la enorme y heterogénea cantidad de información de sus usuarios que recolectan esas plataformas, así como el perfil que se traza de ellos, a través del empleo de algoritmos, con fines comerciales. Las dudas se generan en torno a la preservación de esos datos, pues un eventual empleo de ellos, comprometiendo el anonimato del individuo, constituye un riesgo cierto que genera gran preocupación.

Queda en evidencia, merced a profundas y medulosas investigaciones realizadas en el ámbito académico, el riesgo accesorio de influencia en la conducta del internauta que generan

[7] DAAM: Derechos, Apertura, Accesibilidad y Múltiples Actores.

las redes sociales, incluyendo el mecanismo de "burbuja filtro" y el sesgo de confirmación. Esta cuestión guarda directa relación con la esfera de seguridad, desde el momento en que las redes son vectores de *fake news* y *deep fakes* concebidas y emitidas de modo deliberado, con metas de manipulación.

La posverdad, entendida como una apreciación de la realidad en la cual los hechos concretos ven relativizada su importancia, en función de emociones y creencias personales, no constituye una derivación de las *fake news*. Empero, la influencia de las segundas en la primera es imposible de soslayar. Este vínculo, además, es capitalizado en los procesos de elaboración de acciones de desinformación, donde las narrativas se generan, y los canales de ejecución se seleccionan, en función del blanco seleccionado. Las *fake news* operan a modo de materia prima de las acciones de desinformación, donde elementos de posverdad suelen estar incluidos en forma explícita o velada.

Tanto el abanico de efectos perniciosos que generan ese tipo de noticias, extremadamente heterogéneas en sus formatos, como las acciones de desinformación que se elaboran a partir de ellas, justifican su atención prioritaria desde la perspectiva de la ciberseguridad: desde desestabilizaciones políticas de envergadura, e incluso rupturas de regímenes democráticos, hasta crisis internacionales susceptibles de traspasar el umbral del empleo de la fuerza. La pertinencia de un enfoque de ciberseguridad se reafirma al comprobar que las operaciones de desinformación son empleadas de manera recurrente por diferentes estados hacia otros actores de su ambiente externo, constituyéndose la interferencia rusa en el proceso electoral estadounidense de 2016, un ejemplo paradigmático en cuanto a sus alcances.

Ha quedado planteado en el trabajo que los estados no sólo desarrollan operaciones de desinformación, sino también adoptan posturas de cibersoberanía y despliegan actividades de vigilancia digital de diferente tenor. Las primeras refieren a la regulación del acceso de los ciudadanos a las redes sociales y plataformas digitales, así como del flujo transfronterizo de datos, que hoy afecta a las cuatro quintas partes de los usuarios de Internet en todo el mundo. Las segundas son acciones de amplio espectro que apuntan al monitoreo y control de los ciudadanos, sus conductas y los contenidos que manejan en el dominio digital. La inevitable reflexión, en este punto, gira en torno a la invocación de la seguridad del cuerpo social, incluso del Estado como tal, como justificación para estas conductas restrictivas. En regímenes autoritarios, la vigilancia digital se configura como una herramienta de control social y político menos vinculada con la seguridad que con la ideología, profundamente lesiva a los derechos y garantías individuales.

Pudo constatarse que los alcances de la ciberseguridad se extienden más allá de la ciberguerra, la cibercriminalidad, el ciberterrorismo, la protección de las infraestructuras críticas y otras cuestiones de tratamiento recurrente en este campo. Otros temas menos explorados desde esta perspectiva son igualmente pertinentes, como es el caso de la libertad de acceso a Internet, los riesgos de manipulación de la información existente en la red, con fines de desinformación, y la vulneración de la privacidad del enorme volumen de datos personales que fluyen por ella.

Para concluir, frente al panorama descripto se constata el bajo nivel de institucionalización existente, en el plano internacional. La causa obedece a la ausencia de una convención global de ciberseguridad, producto de la incompatibilidad entre las diferentes lecturas existentes sobre la materia, especialmente entre Occidente y el tándem Rusia-China. Con este

panorama, los mecanismos de gobernanza vigentes apenas alcanzan a uno de los tres tópicos analizados en este trabajo, el de la vigilancia digital y la cibersoberanía. A tono con esa carencia, los desafíos que tiene por delante la comunidad internacional son enormes.

NOTA SOBRE EL AUTOR:

Graduado y Doctor en Relaciones Internacionales (Universidad del Salvador). Tiene un Máster en Sociología, reconocido por la Academia de Ciencias de la República Checa. Realizó estudios posdoctorales en Seguridad Internacional, en la Universidad Complutense de Madrid. Sus principales áreas de expertise giran en torno a la Seguridad Internacional, con énfasis en amenazas no convencionales y transnacionales, seguridad pública en América Latina y ciberseguridad. Ejerció la docencia durante treinta años en diferentes instituciones en niveles de grado, posgrado y doctorado. Ha escrito cuatro libros y colaborado con capítulos en varios otros, además de ser autor de numerosos artículos sobre su especialidad en revistas académicas de diversos países. Actualmente se desempeña como Profesor Permanente (por concurso) en el Colegio Interamericano de Defensa, en Washington. Correo electrónico: mariano.bartolome@iadc.edu

REFERENCIAS

Anguita, Concepción y Bartolomé, Mariano (2021), "El Reto de la Gobernanza Global en Ciberseguridad. La Gestión de la Unión Europea y la Organización de Estados Americanos", en IV Congreso Internacional Comunicación y Pensamiento, Comunicación y política en el mundo digital: tendencias actuales en propaganda, ideología y sociedad, Madrid: Dykinson, en prensa.

Bartolomé, Mariano (2020, 26 de septiembre), "Ciberseguridad: claves para entender su vigencia, dinámica y heterogeneidad en el mundo", *Infobae*.

Boyd, Danah & Ellison, Nicole (2007), "Social Network Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication*, Vol. 13, No. 1, pp. 210-230.

Bradshaw, Samantha & Howard, Phillip (2017), *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Oxford: University of Oxford, Computational Propaganda Research Project

Caldevilla Domínguez, David (2010), "Las Redes Sociales. Tipología, uso y consumo de las redes 2.0 en la sociedad digital actual", *Documentación de las Ciencias de la Información*, No. 33, pp. 45-68.

CCN-CERT (2019), *Desinformación en el ciberespacio*, CCN-CERT BP/13, febrero.

Chaffey, Dave (2021), "Global Social Media Research Summary 2021", *Smart Insights*, March 11.

Chen, Brian (2020, October 20), "It's Google's World. We Just Live in It", *The New York Times*.

Chesney, Robert y Citron, Danielle (2018), "Deep Fakes: ¿una crisis inminente para la seguridad nacional, la democracia y la privacidad?", *Lawfare*, 21 de febrero.

CIGI (2019), *CIGI-Ipsos Global Survey on Internet Security & Trust 2019. Part I & II*.

Cobo, Cristóbal (2019), *Acepto las Condiciones: usos y abusos de las tecnologías digitales*, Barcelona: Fundación Santillana.

Conversia (2020), "¿Qué apps almacenan más datos personales de sus usuarios?", *Conversia*, 21 de diciembre.

Edelman (2018), *2018 Edelman Trust Barometer Report*.

Ford, Elaine (2020), "La desinformación y las fake news en tiempos de Covid-19", en Castillo, Gil y Delgado, Sebastián (Coord.), *Entre información y conspiración*, Montevideo: KAS Oficina Uruguay, pp. 53-63.

— (2021), "Son fake news las fake polls?", *Diálogo Político*, 19 de abril.

Freedom House (2020), *Freedom on The Net 2020. The Pandemic Digital Shadow*, New York: Freedom House

Gady, Franz-Stefan & Austin, Greg (2010), *Russia, the United States and Cyberdiplomacy*, New York: East-West Institute

Galston, William (2020), "Is seeing still believing? The Deepfake Challenge to Truth in Politics", *Brookings Institution*, January 8.

Garro, Gabriela (2016), "Manipulación de redes sociales", *Revista Vacío*, 25 de mayo.

GlobeScan (2017), "Fake Internet Content a High Concern, but Appetite for Regulation Weakens", *Press Release*, September 21.

Gold, Josh (2019), "Two Incompatible Approaches to Governing Cyberspace hinder Global Consensus", *Leiden Security and Global Affairs*, May 16.

Hoogensen Gjørv, Gunhild (2020), "Coronavirus, invisible threats and preparing for resilience", *NATO Review*, May 20.

Hypponen, Mikko (2014), "Ciberataques", en Open Mind & BBVA (Eds.), *Cambio. 19 ensayos fundamentales sobre cómo Internet está cambiando nuestras vidas*, Madrid: BBVA, pp.102-123

IAB Spain (2019), *Estudio Anual de las Redes Sociales*, Madrid: Asociación de Publicidad, Marketing y Comunicación Digital en España.

Jaimovich, Desirée (2019, 13 de octubre), "Ya hay redes sociales que tienen más habitantes que los países más poblados del planeta", *Infobae*.

Jaitner, Margarita (2013), "Exercising Power in Social Media", en Rantapelkonen, Jari & Salminen, Mirva (Eds.), *The Fog of Cyber Defense*, Helsinki: National Defense University, pp. 57-76.

Karanicolas, Michael (2014), *Travel Guide to the Digital World: Surveillance and International Standards*, London: Global partners Digital.

Kemp, Simon (2021), "Digital 2021: Global Overview Report", *Datareportal*, January 27.

Kissinger, Henry (2016), *Orden Mundial*, Barcelona: Debate

Le Pan, Nicholas (2020), "Visualizing the Length of the Fine Print, for 14 Popular Apps.", *Visual Capitalist,* April 18.

Lissardy, Gerardo (2017, 9 de abril), "Despreparada para a era digital, a democracia está sendo destruída, afirma guru do 'big data'", *BBC Mundo*.

Lozano, Alberto (2020), "Posverdad y Relaciones Internacionales", *Foreign Affairs Latinoamérica,* octubre.

Mac Farquhar, Neil (2018, February 18), "Inside the Russian Troll Factory: Zombies and a Breakneck Pace", *The New York Times*.

Magnani, Esteban (2020), "El capitalismo actual es de vigilancia", *Nueva Sociedad,* Julio.

Malaspina, Lucas (2020), "¿Hacia un mundo felizmente vigilado?", *Nueva Sociedad,* abril.

Marcos Recio, Juan, Sánchez Vigil, Juan y Olivera Zaldúa, María (2017), "La enorme mentira y la gran verdad de la información en tiempos de la posverdad", *Scire*, Vol. 23, No. 2, pp.13-23.

Merino, Marcos (2021), "Un boicot masivo a H&M en China borra casi por completo de su Internet al mayor vendedor de 'moda rápida' del mundo", *Genbeta,* 26 de marzo.

Monleón-Getino, Antonio (2015), "El impacto del Big data en la Sociedad de la Información. Significado y utilidad.", *Historia y Comunicación Social,* Vol. 20, No. 2, pp. 427-445.

Monnerat Lot, Yuri y Barros Cianconi, Regina (2018), "Vigilância e privacidade, no contexto do Big Data e dados pessoais: análise da produção da Ciência da Informação no Brasil", *Perspectivas em Ciência da Informação,* Vol. 23, No. 4, pp. 117-132.

Morales, Samuel (2019), "Guerra informativa: llenar la información de desinformación", *Instituto Español de Estudios Estratégicos (IEEE),* Documento de Opinión 45/2019, 27 de mayo.

Muñoz, Juan (2011, 9 de junio), "El acceso a Internet, un derecho humano según la ONU", *CNN en español*.

Nye, Joseph (2010), *Cyber Power,* Belfer Center for Science and International Affairs, May.

Organización Mundial de la Salud (2020), "Inmunizar al público contra la desinformación", *Boletín OMS*, 25 de agosto.

Ortiz-Ospina, Esteban (2019), "The Rise of Social Media", *Our World in Data,* September 18.

Payo, Alberto (2018), "Casi el 90% de las apps envía sus datos a una empresa propiedad de Alphabet", *Applicantes,* 26 de octubre.

Peirano, Marta (2019), *El Enemigo conoce el Sistema,* Madrid: Debate.

Quintana, Yolanda (2016), *Ciberguerra*, Madrid: Ediciones de la Catarata.

Rathi, Sanjana (2020), "Weaponization of Social Media Platforms in Post-Truth Era", *The Cyber Diplomat,* March 3.

Redondo, Mónica (2017), "Publican los anuncios comprados por Rusia en Facebook", *Hipertextual*, 2 de noviembre.

REUTERS (2010, 8 de marzo), "Internet, un 'derecho humano' para cuatro de cada cinco usuarios", *El Mundo*.

Rey, Fernando (2020), "El Big Data, o cómo tus datos le han dado más poder a la economía y la política", *El Orden Mundial*, 26 de enero.

Riordan, Shaun (2019), "El mundo 'deepfake' también necesita diplomáticos", *EsGlobal*, 8 de mayo.

Rojas Caja, Fernando (2020), "El Fact Checking. Las agencias de verificación de noticias en España", *Instituto Español de Estudios Estratégicos (IEEE)*, Documento de Opinión 89/2020, 19 de junio.

Rozpedowski, Joanna (2021), "Digital Sovereignty in an Era of Global Surveillance, Disinformation and Info-demics", *Geopolitical Monitor*, May 17.

Sampedro Oliver, Raúl (2021), "Redes sociales: desinformación, adicción y seguridad", *Instituto Español de Estudios Estratégicos (IEEE)*, Documento de Opinión 30/2021, 9 de marzo.

Santiago Gómez, Elvira y Rodríguez Rodríguez, Carmen (2018), "Tecnologías de la vigilancia: una mirada hacia la violencia legítima del estado en cuestiones de seguridad y control", *Encrucijadas: Revista Crítica de Ciencias Sociales*, No. 16, pp. 1-17.

Souter, David y Van der Spuy, Anri (2018), *Indicadores de la UNESCO sobre la universalidad de Internet: Marco para la evaluación del desarrollo de Internet*, Paris: UNESCO.

Stang, Gerald (2013), "Global Commons. Between Cooperation and Competition", European Union Institute for Security Studies, *Issue Brief*, No. 17, April.

Timberg, Craig & Romm, Tony (2018, December 17), "New Report on Russian Disinformation, Prepared for the Senate, Shows the Operation's Scale and Sweep", *The Washington Post*.

Toews, Rob (2020, 25 de mayo), "Los deepfakes van a causar estragos en la sociedad. No estamos preparados", *Forbes*.

Tsaruk, Oleksandr & Korniiets, Maria (2020), "Hybrid Nature of Modern Threats to Cybersecurity and Information Security", *Smart Cities and Development Journal*, Vol. 4, No. 11, pp. 57-78.

UIT (2010), "Decisiones destacadas de Guadalajara", Actualidades de la UIT 9/2010, pp. 20-22.

— (2020), "Inteligencia Artificial para el bien", *Documentos de antecedentes temáticos*, octubre.

UNCTAD (s/f), *Global Cyberlaw Tracker*.

— (2019), *Informe sobre la Economía Digital 2019*, New York: United Nations Publications.

UNESCO (2018), *Tendencias mundiales en libertad de expresión y desarrollo de los medios: informe mundial 2017/2018*, París: UNESCO.

— (2020), "Periodismo, libertad de prensa y Covid-19", *Serie de la UNESCO: Tendencias mundiales en libertad de expresión y desarrollo de los medios de comunicación*.

United Nations (2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue,* A/HRC/17/27, May 16.

Urgessa, Worku (2020), "Multilateral Cybersecurity Governance: Divergent Conceptualizations and its Origin", *Computer Law & Security Review*, No. 36, pp. 1-8.

Yuan, Li (2019, 5 de enero), "Así funciona una fábrica de censura en China", *The New York Times en español*.