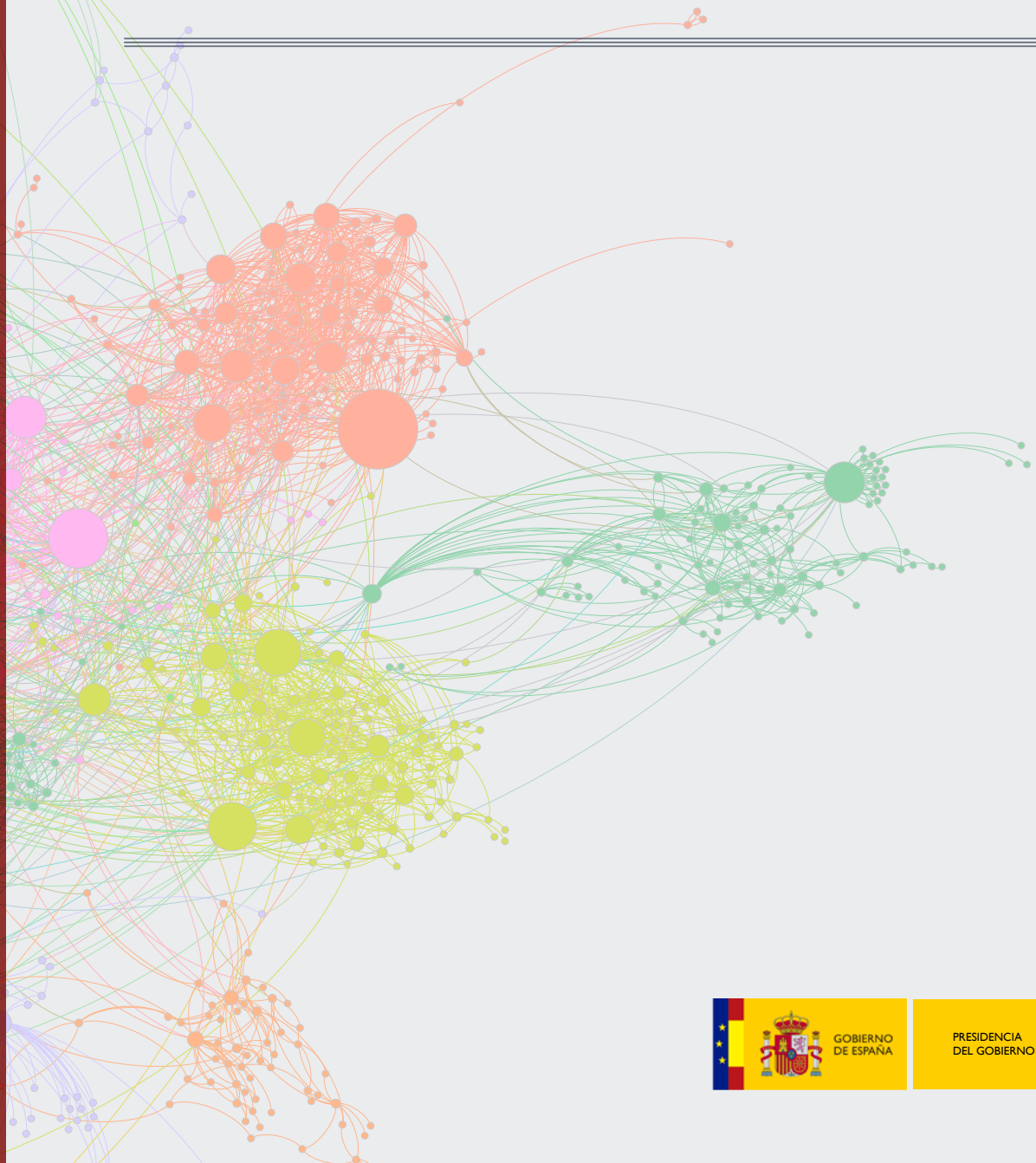
LUCHA CONTRA LAS CAMPAÑAS DE DESINFORMACIÓN EN EL ÁMBITO DE LA SEGURIDAD NACIONAL

Propuestas de la sociedad civil



GOBIERNO DE ESPAÑA
PRESIDENCIA DEL GOBIERNO

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES Y MEMORIA DEMOCRÁTICA

NIPO (edición on-line): 089220215
Fecha de edición: Septiembre 2022
Imprime: Solana e Hijos, Artes Gráficas S.A.U.

LUCHA CONTRA LAS CAMPAÑAS DE DESINFORMACIÓN EN EL ÁMBITO DE LA SEGURIDAD NACIONAL

Propuestas de la sociedad civil

Los expertos participantes en los Grupos de Trabajo lo son a título personal y no a título institucional. Por lo tanto, sus opiniones y recomendaciones no representan ni comprometen a las instituciones a las que pertenecen.

El resultado de los trabajos es producto de un ejercicio de reflexión colectivo, si bien, no tiene por qué representar la opinión individual de todos los participantes ni de las organizaciones o entidades representadas, quienes no necesariamente comparten todas las conclusiones o propuestas.

PRESENTACIÓN

Las campañas de desinformación constituyen una grave amenaza para la seguridad nacional. En los estudios prospectivos llevados a cabo en análisis de riesgos, las campañas de desinformación figuran entre los factores que presentan una tendencia a empeorar a corto y medio plazo.

La Estrategia de Seguridad Nacional 2021 - "un proyecto compartido" incluye este fenómeno en el diagnóstico del panorama de amenazas para la seguridad nacional, por el amplio potencial que presenta para generar confusión informativa y desconfianza en las instituciones, así como para minar la cohesión social.

En los últimos años, los estados democráticos se han visto afectados por distintas campañas de desinformación, con origen o alentadas por actores extranjeros y a menudo replicadas y amplificadas por actores nacionales de forma más o menos intencional. Dichas campañas se focalizaron en afectar procesos electorales, minar la confianza de la ciudadanía en las instituciones en circunstancias excepcionales, como fue el caso de la pandemia de la COVID-19, así como en fomentar de manera preocupante la polarización y fragmentación social.

Estos trabajos, de carácter conceptual en su mayor parte y orientación divulgativa, tienen por principal objetivo contribuir a un mejor entendimiento del fenómeno de la desinformación, desde una aproximación colaborativa público-privada, desarrollado entre la sociedad civil, cuyos representantes en los distintos grupos de trabajo aglutinan un profundo conocimiento del tema, y los sectores de la Administración pública claramente implicados, todo ello a través del análisis, debate, crítica constructiva y consenso.

En base a todo lo anterior, desde el Departamento de Seguridad Nacional resulta obligatorio que esta publicación dedique sus palabras de apertura a agradecer la generosa y desinteresada contribución de todos aquellos autores que, con su conocimiento, dedicación, esfuerzo desinteresado y experiencia, la han hecho posible.

Miguel Ángel Ballesteros Martín
Director del Departamento de Seguridad Nacional
Presidencia del Gobierno

RESUMEN EJECUTIVO

RESUMEN EJECUTIVO

Los derechos y libertades fundamentales, a nivel europeo, consagrados en la Carta de los Derechos Fundamentales de la Unión, y a nivel nacional, en la Constitución española, son los cimientos sobre los que se asientan las actuales sociedades democráticas y de Derecho. El ejercicio real de la democracia sólo puede prosperar en un clima de respeto a las libertades de pensamiento, información y expresión, de tal modo que cada ciudadano sea libre para formar y expresar sus propias opiniones, pudiendo así tomar parte en el debate social y político.

La transformación digital desarrollada durante las últimas décadas, en concreto en lo referente al espacio informativo, viene a ofrecer nuevas y excelentes oportunidades para la participación democrática, si bien también ha puesto de manifiesto nuevas e importantes vulnerabilidades, algunas de las cuales han facilitado la proliferación de campañas de desinformación, de elevado impacto y potencial amenaza para la seguridad nacional.

Las campañas de desinformación, en el ámbito de la seguridad nacional son entendidas como patrones de comportamiento desarrollados en el dominio informativo, llevados a cabo de forma coordinada e intencional, cuya implantación y difusión supone una amenaza para los valores constitucionales, los procesos democráticos, las instituciones democráticamente constituidas y, por ende, para la seguridad nacional.

La Unión Europea, en diciembre del año 2018, ya resaltó la necesidad de abordar esta amenaza en su *Plan de Acción contra la desinformación*, en el que se resalta que: «una respuesta integral a la desinformación requiere la participación activa de la sociedad civil». Así mismo este Plan destaca que, para poder afrontar este reto, se requiere: «una mejor comprensión de las fuentes de desinformación y de las intenciones, herramientas y objetivos subyacentes a la desinformación, pero también de nuestra propia vulnerabilidad».

Posteriormente, en diciembre del año 2020, la Unión Europea vuelve a incidir en la amenaza de la desinformación en el *Plan de Acción para la Democracia Europea*, en el que se alerta a los Estados miembros del riesgo que suponen las campañas de desinformación, tanto para la seguridad de las instituciones europeas y la de los Estados Miembros, como para la integridad de los valores y procesos democráticos del conjunto de Europa. De nuevo, a nivel europeo se destaca la necesidad que los Estados miembros incidan en un conocimiento profundo de la amenaza y se urge a una cooperación más estrecha con las partes implicadas de la sociedad civil, el mundo académico y la industria.

En este contexto, a finales del año 2020 el Departamento de Seguridad Nacional reunió a un grupo de expertos de la sociedad civil, incluyendo periodistas, académicos, representantes de centros de pensamiento y análisis, organizaciones sociales y de las plataformas digitales, para que, junto a representantes de la Administración Pública, llevaran a cabo un esfuerzo conjunto de análisis tanto de la amenaza que supone el fenómeno de la desinformación, como de las posibles estrategias para detectarla, hacerle frente y garantizar, por tanto, la indemnidad de los valores democráticos y las libertades y derechos fundamentales.

En el seno de este grupo de expertos se constituyeron a su vez cinco grupos para el desarrollo de los trabajos que aquí se presentan en sus respectivos Capítulos. El objetivo de estos trabajos es el de analizar las diferentes dimensiones desde las que se puede abordar y afrontar el fenómeno de la desinformación: desde la contextualización y definición de la amenaza hasta la necesidad de fomentar la alfabetización mediática, pasando por la evaluación del marco normativo y perspectivas de futuro en el ámbito de la regulación, la especial vulnerabilidad de los procesos electorales y, por último, la necesidad de desarrollar una estrategia nacional contra la desinformación para dar una respuesta coordinada y eficaz a esta amenaza.

El periodo de tiempo durante el que se desarrollaron los trabajos referidos transcurrió durante un año, entre finales del año 2020 y finales del año 2021, por lo que los Capítulos no incluyen referencias temporales más allá de la fecha de finalización, no incorporan referencia alguna a la invasión rusa de Ucrania (febrero 2022) ni a las lecciones hoy aprendidas a causa de esta crisis bélica en el ámbito de la desinformación.

Pese a ello, es necesario recalcar que, los niveles de desinformación y manipulación informativa observados en torno a este acontecimiento bélico, con clara afectación a la Unión Europea y sus Estados miembros, incluida España, han contribuido notablemente a poner de manifiesto, aún más, la

necesidad que tienen las sociedades democráticas de desarrollar mecanismos para dar respuesta a las campañas de desinformación y salvaguardar los valores y procesos democráticos y los intereses de seguridad nacional.

En este sentido, el contenido de los trabajos, sus propuestas y reflexiones, aun habiendo sido desarrolladas antes del inicio de la mencionada invasión, son ahora más oportunas y necesarias que nunca para avanzar en cada uno de los ámbitos analizados.

La importancia de estos trabajos fue reconocida en la Estrategia de Seguridad Nacional de 2021, aprobada en diciembre de 2021, la cual subraya la relevancia de la amenaza de las campañas de desinformación para los procesos electorales y destaca su gran potencial para polarizar a la sociedad y minar su confianza en las instituciones. Además, viene a confirmar la extraordinaria necesidad de contar con la colaboración público-privada en el desarrollo de medidas de detección y respuesta, entre las que se incluye la imprescindible sensibilización y formación ciudadana en relación con el fenómeno de la desinformación.

En este contexto el pasado 31 de mayo de 2022, el Consejo de Ministros aprobó la creación del *Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional*. La constitución formal de este Foro, como órgano colegiado, viene a dar continuidad a los trabajos y aportaciones llevadas a cabo por los distintos representantes de la sociedad civil que conformaron el grupo de expertos a cuya autoría corresponden estos trabajos.

Los trabajos se estructuran del siguiente modo:

CAPÍTULO 1: "La desinformación: una amenaza a la democracia"

Las campañas de desinformación, debido a su potencial para corromper el debate público, erosionar la confianza en las instituciones, manipular a la opinión pública y condicionar la política exterior, representan una amenaza para las sociedades democráticas. De hecho, es una de las estrategias a las que recurren habitualmente las potencias extranjeras hostiles en operaciones de injerencia para socavar el buen funcionamiento de las instituciones. Para permitir identificar y poder combatir la desinformación es importante disponer de una definición precisa.

En este capítulo los autores se remiten a la definición del Comité de Expertos de Alto Nivel de la Unión Europea, que describe la desinformación como «la información verificablemente falsa o engañosa que se crea, presenta y divulga

con fines lucrativos o para inducir a error deliberadamente a la población, y que puede causar un perjuicio público».

CAPÍTULO 2: "Propuestas de regulación ante la desinformación"

La regulación de este fenómeno es extraordinariamente compleja y sensible, por cuanto se ven afectados elementos básicos del sistema democrático como son las libertades informativas de los ciudadanos, redes, plataformas y medios de comunicación. En este sentido, toda regulación española ha de partir de las importantes acciones y regulaciones que se vienen desarrollando desde la Unión Europea.

En este contexto, se aprecian positivamente los modelos corregulatorio y autorregulatorio, que permiten conciliar los objetivos de lucha contra la desinformación con la preservación de las libertades informativas y de prensa de los distintos sujetos implicados. En este capítulo se tiene muy cuenta la intensa labor de las plataformas y se valora el papel de los medios y verificadores, respecto de los que se apuntan posibles líneas de regulación. Sobre estas bases, en el capítulo se proponen mejoras para la regulación institucional y orgánica en el ámbito de la lucha contra la desinformación, en la línea de una necesaria transparencia e integración de la sociedad civil. También se recogen propuestas de mejora relativas a las amenazas internacionales, a la ciberdefensa y a la cooperación con la UE. En el ámbito electoral, siguiendo recientes pronunciamientos del Tribunal Supremo, se brindan posibles mejoras, entre ellas, respecto de las competencias de la Junta Electoral, la publicidad electoral o en el ámbito más concreto de la protección de datos para las plataformas.

CAPÍTULO 3: "La alfabetización mediática, herramienta clave en la lucha contra la desinformación"

En un mundo cada vez más digitalizado, la alfabetización mediática desempeña un papel clave para contrarrestar el fenómeno de la desinformación, que, si bien no distingue por edad, ni estrato social, afecta particularmente a los grupos más vulnerables, como las personas en riesgo de exclusión social o quienes no tienen formación en competencias digitales.

La alfabetización mediática e informacional es clave para que las personas puedan desarrollar su capacidad crítica y emitir juicios equilibrados a partir de la información que reciben. Este capítulo expone la importancia de fomentar iniciativas innovadoras en este campo y desglosa muchas ya desarrolladas

por medios de comunicación, verificadores, redes sociales, organizaciones e instituciones.

Los expertos participantes en este capítulo consideran imprescindible incluir la alfabetización mediática como una asignatura específica en el currículum académico en todos los niveles educativos. Es necesario dotar a los alumnos, en todos los niveles, de conocimientos sobre la repercusión de los mensajes para detectar, impedir su difusión y, en su caso, eliminar los discursos de odio y promover una cultura de encuentro, convivencia y paz. En una dimensión más social, también parece adecuado trabajar en el diseño de campañas de concienciación que ayuden a la ciudadanía a estar alerta.

CAPÍTULO 4: "Propuestas para combatir las campañas de desinformación en procesos electorales"

Las campañas de desinformación suponen una grave amenaza para los procesos electorales. Su peligro radica en su posible influencia en los resultados de unas elecciones y, sobre todo, en sus efectos estructurales como la polarización de la sociedad o la desconfianza y deslegitimación de los procesos e instituciones democráticas. La lucha contra la desinformación en las elecciones exige el trabajo coordinado de la sociedad civil y los servidores públicos del Estado a través de tres pilares esenciales: la información y transparencia, la formación o alfabetización mediática y la prevención.

Sobre estos pilares, en este capítulo se recogen una serie de recomendaciones o sugerencias a diferentes actores del proceso electoral como son la Administración Pública y el legislador, las Juntas Electorales y Tribunal de Cuentas, los partidos políticos, las plataformas digitales y los medios de comunicación y verificadores. Se incluyen también recomendaciones sobre ciberseguridad destinadas a combatir la desinformación.

La evolución de la tecnología y de nuestra propia sociedad exige una revisión constante de la materia. Por ello, una de las conclusiones incide en la necesidad de disponer de un foro estable de encuentro, contacto, comunicación y trabajo que permita enfrentarse a cada proceso electoral desde una perspectiva integral.

CAPÍTULO 5: "Principios para una estrategia contra la desinformación"

La desinformación, a granel o empaquetada en campañas, ha sido identificada como una amenaza que plantea riesgos, tanto a escala nacional como internacional, y cuya estrategia de neutralización requiere la definición de principios para el empleo de nuevas capacidades, que rebasan las que caracterizan los instrumentos convencionales hasta ahora disponibles.

En este capítulo se trata de evaluar la gravedad de los daños que pueden causar las distintas modalidades de desinformación y de describir las medidas que, en aras de contrarrestarlas, ya están adoptando terceros países y agentes no estatales. Interesa observar cómo el mero anuncio de que se procedería a este análisis suscitó un amplio debate político, social y mediático, propiciado por la sana sospecha de que, con el propósito de defender la vigencia del sistema democrático actual, pudiera erosionarse el intangible de los derechos y libertades fundamentales -de prensa, de expresión y de difusión-.

Desde esta sensibilidad acuciante de conjugar que una futura Estrategia contra la desinformación y las medidas que se propongan contribuyan a la solución del problema descrito, se asume la obligación de su elaboración en unos términos que permitan su encuadre en el escrupuloso respeto a los principios básicos que nos distinguen, que aseguren su estricta coherencia jurídica con los derechos y obligaciones constitucionales y con las iniciativas europeas avanzadas, que preserven el derecho a la legítima defensa de la seguridad nacional, y que garanticen la participación de los actores privados y de la sociedad civil, a partir de su imprescindible alfabetización mediática.

ÍNDICE

CAPÍTULO 1

LA DESINFORMACIÓN: UNA AMENAZA A LA DEMOCRACIA

Coordinador sociedad civil:

Pablo Hernández Escayola (Maldita)

Coordinador institucional:

Ministerio de Asuntos Exteriores, Unión Europea y Cooperación

Autores y colaboradores:

José Ignacio Torreblanca Payá (European Council on Foreign Relations)

Guillermo Serrano Peña (Facebook)

Manuel Castro Mengibar (Federación de Asociaciones de Radio y Televisión)

Ana Abade Gil (Google)

Santiago Menéndez-Abascal Cabiedes (Google)

Manuel Ricardo Torres Soriano (Instituto de Seguridad y Cultura)

Yolanda Quintana Serrano (Plataforma en Defensa de la Libertad de Información)

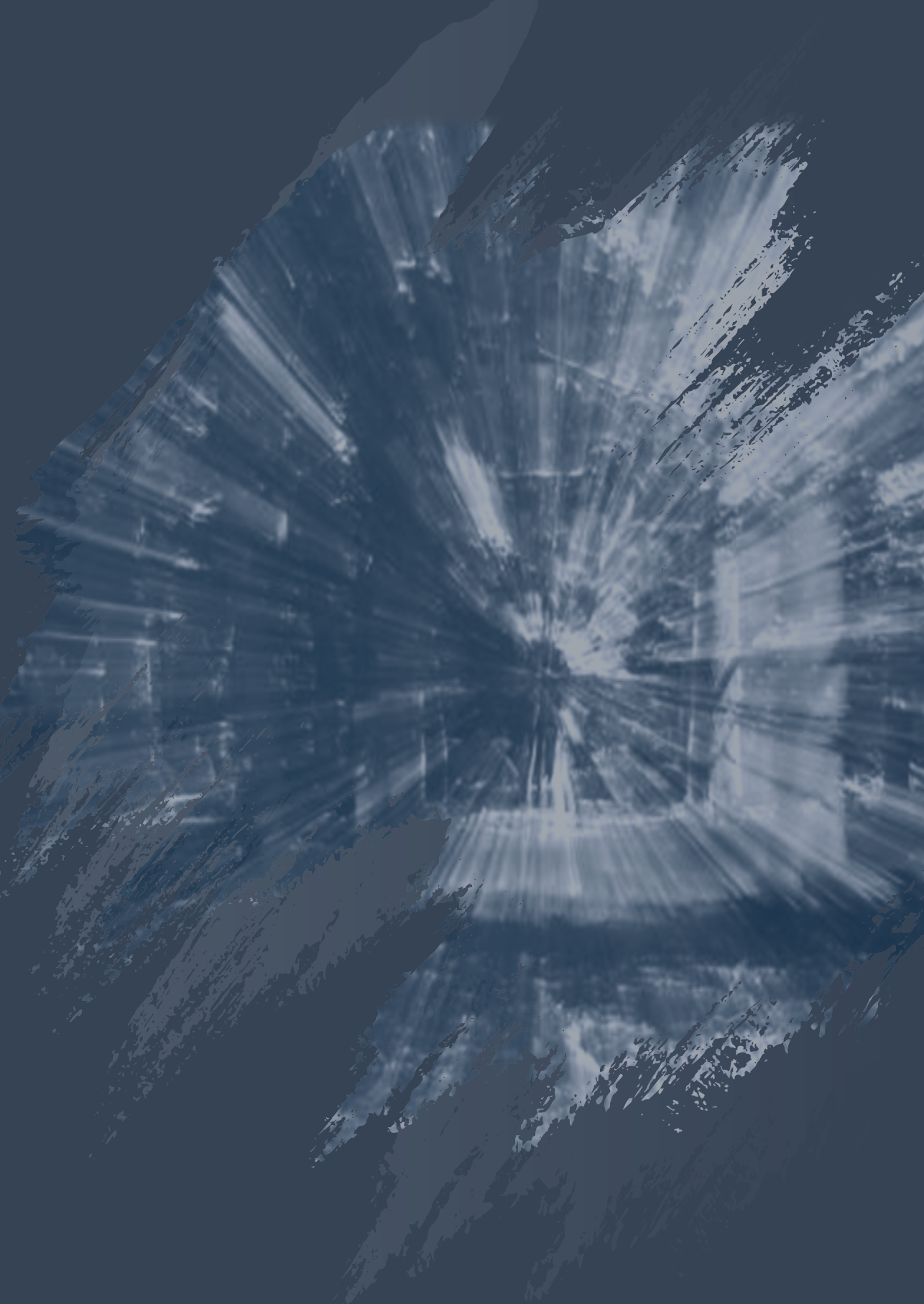
Ángel Badillo Matos (Real Instituto Elcano)

Camino Rojo Torres (Twitter)

Javier Jordán Enamorado (Universidad de Granada)

Ramón Salaverría Aliaga (Universidad de Navarra)

Guillem Colom Piella (Universidad Pablo de Olavide)



INTRODUCCIÓN

Uno de los elementos que distingue a las democracias de las dictaduras es el lugar que ocupan la verdad y la mentira: las democracias se articulan en torno a la verdad, las dictaduras en torno a la mentira. Para poder existir, las democracias requieren un espacio público basado en la confianza y la creencia en la posibilidad de establecer la verdad de los hechos. Por el contrario, las dictaduras no pueden sobrevivir a la exposición a los hechos, por lo que necesitan destruir la verdad y sustituir el espacio público por la propaganda. Eso explica por qué las democracias necesitan medios de comunicación independientes del poder político mientras que, por el contrario, las dictaduras los prohíben y centralicen la producción y difusión de información. También permite entender por qué cuando los medios de comunicación entran en crisis y no son capaces de cumplir su función, la democracia también lo hace.

En una democracia, la ciudadanía necesita disponer de información veraz para poder evaluar las acciones de sus gobernantes y hacerlos rendir cuentas por ellas. Esa función de contrapoder explica por qué tan a menudo se describe a los medios de comunicación como el "cuarto poder" y por qué las Constituciones democráticas establecen y garantizan la libertad de prensa e información como un pilar central. Así, el artículo 19 de la Declaración Universal de Derechos Humanos establece que todo individuo tiene derecho a "[..] recibir informaciones y opiniones y difundirlas sin limitación de fronteras, por cualquier medio de expresión". Por su parte, la Constitución española, establece en su artículo 20 el derecho "a comunicar o recibir libremente información *veraz* por cualquier medio de difusión" así como la prohibición absoluta de "restringir el ejercicio de estos derechos mediante ningún tipo de censura previa".

La Constitución española, establece en su artículo 20 el derecho "a comunicar o recibir libremente información veraz por cualquier medio de difusión" así como la prohibición absoluta de "restringir el ejercicio de estos derechos mediante ningún tipo de censura previa".

En la actualidad, Internet, el desarrollo de la web, de la sociedad de la información y las nuevas tecnologías permiten un acceso a información y conocimiento a una escala e intensidad sin precedentes. La innovación ha permitido el desarrollo de tecnologías idóneas para compartir ideas y opiniones, tomar parte en debates y procesos democráticos y, en general, disfrutar y ejercer eficazmente derechos fundamentales y libertades públicas como nunca antes en la historia de la humanidad.

Gracias a las innovaciones digitales, los ciudadanos tienen la capacidad de acceder a información, servicios y herramientas que antes eran escasas o inaccesibles debido a limitaciones económicas, geográficas o físicas. Esto ha creado libertades sin precedentes para las comunidades de todo el mundo. Pese a ello, las democracias contemporáneas experimentan una crisis prolongada y profunda. De acuerdo con los principales indicadores internacionales Freedom House 2021 (Repucci y Slipowitz, 2021), esta crisis tiene un carácter global y afecta tanto a la cantidad como a la calidad de las democracias. Este declive democrático, que dura ya quince años, obedece tanto a causas materiales (relacionadas con las crisis económicas y el consiguiente aumento de las desigualdades) como afectivas (relacionadas con la emergencia de los sentimientos de agravio personal y colectivos), y es particularmente visible en el incremento de la desafección y desconfianza hacia las instituciones centrales de la democracia, incluyendo los medios de comunicación.

Un elemento común a esa crisis democrática tiene que ver con la desintermediación favorecida por la emergencia de las redes sociales y el consiguiente debilitamiento de los medios de comunicación tradicionales. Estos, al igual que los partidos políticos tradicionales y otros actores han ido perdiendo capacidad de articular el debate público y la demanda de la ciudadanía de recibir información veraz y contrastada. La revolución digital y de las tecnologías de comunicación ha favorecido la emergencia de un ágora virtual paralelo al conformado en el pasado por partidos políticos, parlamentos y medios de comunicación. Debido a la facilidad de acceso, bajo coste y alcance masivo e inmediato de los contenidos que permite la tecnología digital, esa ágora virtual, al tiempo que ha venido a ofrecer a la ciudadanía amplísimas posibilidades de actuar y compartir información de forma horizontal y sin intermediarios, se ha mostrado vulnerable a la manipulación de la información y los sentimientos de la ciudadanía.

La revolución digital ha favorecido la emergencia de un ágora virtual paralelo al conformado en el pasado por partidos políticos, parlamentos y medios de comunicación.

Aprovechando la eventual debilidad o inadecuación de las normas que regulan las redes sociales y el desconocimiento y buena fe del público, actores malintencionados de origen interno o externo (o en ocasiones ambos trabajando al unísono) han empleado las redes sociales para, mediante operaciones de influencia y desinformación cuidadosamente planificadas y ejecutadas, debilitar la confianza del público en las instituciones democráticas y los medios de comunicación (Torreblanca, 2020). Esas operaciones han buscado influir en los procesos electorales democráticos, alentando un clima de polarización que favorezca a opciones políticas populistas o extremistas de marcado contenido iliberal. También han perseguido debilitar la confianza de la ciudadanía en las principales instituciones políticas y sociales, como hemos visto durante la pandemia de la COVID-19 con el intento de desacreditar a científicos y expertos.

Como han acreditado las investigaciones del Servicio Europeo de Acción Exterior de la Unión Europa (SEAE) y de las propias plataformas tecnológicas (Facebook, 2021), un gran número de esas campañas han estado inspiradas o apoyadas por regímenes autoritarios que rivalizan estratégicamente con la UE y sus miembros, así como con otros estados democráticos. Para dichas potencias extranjeras, las operaciones de influencia y desinformación tienen un doble atractivo: por un lado, debilitan a las democracias y, por tanto, su capacidad de hacerles frente; por otro, intentan mostrar a sus ciudadanos que las democracias no funcionan y que, por tanto, no representan una alternativa válida a sus regímenes.

Un gran número de esas campañas han estado inspiradas o apoyadas por regímenes autoritarios que rivalizan estratégicamente con la UE y sus miembros, así como con otros estados democráticos.

Las consecuencias de estas campañas y vulnerabilidades han sido tan amplias como visibles tanto en los intentos de influir en las campañas electorales, impulsando fuerzas y narrativas extremas como en el impulso de la polarización política y la desconfianza en las instituciones. El Barómetro Edelman, que mide la evolución de la confianza en 28 países del mundo, viene detectando una caída sostenida de la confianza de la ciudadanía en la política y los medios de comunicación, especialmente en las redes sociales, que son aquellas en la que menos confía la ciudadanía (Edelman, 2021). Por su parte, en el Eurobarómetro Flash 464, de febrero de 2018, elaborado por la Comisión Europea, al menos la mitad de los encuestados afirmó haber estado expuesto a noticias falsas una vez a la semana, mientras que un 83% manifestó creer que las noticias falsas suponían un peligro para la democracia (Comisión Europea, 2018).

La desinformación es un problema complejo que va mucho más allá de las noticias falsas. Como se ha expuesto, detrás de ellas encontramos elementos como las tensiones geopolíticas entre democracias y regímenes autoritarios; la naturaleza abierta y horizontal del ecosistema digital; las dificultades técnicas a la hora de regular las redes sociales y moderar sus contenidos; las divergencias en las diferentes concepciones de los límites de la libertad de expresión dentro de cada democracia y entre ellas; la crisis de la democracia representativa; la debilidad de los medios de comunicación tradicionales; los problemas de concentración de mercado o la inexperiencia de muchos usuarios. Estas son, por tanto, el resultado de un proceso complejo que requiere tratarse de forma integral si se quiere atajar de forma efectiva. Pero para poder diseñar estrategias efectivas, primero hay que conocer el fenómeno en profundidad.

Foto 1: Banderas de la Unión Europea ondean ante la sede de la Comisión Europea en Bruselas (Bélgica) Pixabay/NakNakNak

Afortunadamente, las democracias están reaccionando. La toma de conciencia acerca de este problema ha abierto un proceso de actuación en múltiples ámbitos. La Comisión Europea no solo ha puesto en marcha un programa de acción de defensa de la democracia (Comisión Europea, 2020) cuyo fin es ayudar a las democracias a protegerse sino que ha impulsado, de acuerdo con el Consejo Europeo, una estrategia de lucha contra la desinformación que involucre a todos los estados miembros (Comisión Europea 2018). Gobiernos y parlamentos, apoyándose en expertos, organismos regulatorios e instituciones de la sociedad civil y del mundo empresarial, incluidos los propios medios de comunicación y las redes sociales y plataformas tecnológicas han iniciado un proceso de discusión acerca de la mejor manera de regular la moderación de contenidos ilícitos o dañinos y las responsabilidades de los diferentes actores.

Por otro lado, se han puesto en marcha iniciativas de educación y sensibilización para mejorar la capacidad de la ciudadanía de detectar y rechazar las informaciones falsas que trasladan dichas campañas de desinformación. Al mismo tiempo, se está estudiando cómo lograr una mejor coexistencia entre medios de comunicación tradicional y redes sociales, de tal manera que podamos preservar el papel central de unos medios de comunicación de calidad como elemento de fortaleza democrática. Por su parte, los gobiernos democráticos también están actuando a la hora de denunciar las operaciones de influencia originadas en terceros países, coordinándose para responder y disuadir a los gobiernos que las impulsan e impedir que dichos países puedan, amparándose en la manipulación de las redes sociales y sus medios de comunicación oficiales o controlados por ellos, pero aparentemente independientes, diseñar y emprender operaciones de guerra híbrida contra las democracias.

RIVALIDAD ENTRE GRANDES POTENCIAS: CONFLICTOS EN LA ZONA GRIS Y ESTRATEGIAS HÍBRIDAS

Uno de los motivos que explica las campañas de desinformación tiene que ver con el contexto internacional, en concreto con la rivalidad creciente entre grandes potencias. Como el coste de un enfrentamiento armado directo es sumamente elevado, el antagonismo entre ellas se canaliza a través de instrumentos de poder más sutiles, incluidos los de carácter informativo. En la literatura especializada, la conflictividad por debajo del umbral de la guerra se conoce como zona gris. Con ese término se alude a un espacio intermedio en el espectro del conflicto político que separa la competición acorde con las pautas convencionales de la política entre Estados, del enfrentamiento armado directo y continuado. El actor que recurre a la zona gris trata de alcanzar sus objetivos mediante el ejercicio de la coerción y la degradación del proceso de toma de decisiones políticas de su rival, aplicando gradualmente estrategias multidimensionales y sincronizadas, también conocidas como híbridas (Jordán, 2018).

En la literatura especializada la conflictividad por debajo del umbral de la guerra se conoce como zona gris, un espacio intermedio en el espectro del conflicto político que separa la competición acorde con las pautas convencionales de la política entre Estados, del enfrentamiento armado directo y continuado.

Conviene destacar tres aspectos del conflicto en la zona gris para entender el rol que desempeñan las campañas de desinformación:

- **Ambigüedad**: ni relaciones pacíficas ni conflicto armado. El carácter fundamentalmente no violento del conflicto –salvo episodios puntuales y con empleo limitado de la violencia– es intencionado por parte de quien lo instiga. Se evita cruzar líneas rojas que provoquen una escalada militar con costes altamente elevados y consecuencias imprevisibles. Al librarse por debajo del umbral de la guerra, la verdadera dificultad a la hora de identificar la zona gris se encuentra en el otro extremo, al tratar de diferenciar el conflicto en la zona gris de lo que se podría entender como competencia pacífica acorde con el decoro, competencia bona fide, etc. En definitiva, de la política internacional que discurre dentro de parámetros ampliamente aceptados. Se trata de criterios inevitablemente subjetivos; y en ello radica precisamente una característica de esta opción estratégica:

su ambigüedad. Una ambigüedad intencionada que dificulta tanto la identificación de las actividades hostiles, como la articulación de estrategias de respuesta.

- **Gradualismo**: El planteamiento del conflicto por parte de quien lo instiga suele ser a largo plazo por lo que abundan las acciones interconectadas y concebidas para alcanzar ganancias de manera paulatina. El gradualismo pretende evitar reacciones contundentes manipulando el umbral de respuesta del oponente mientras va modificando a su favor la situación estratégica por suma de efectos. El gradualismo refuerza la ambigüedad, pues la gravedad y la interrelación de las distintas acciones no siempre resulta obvia a los decisores políticos del rival, a sus aliados y a sus respectivas opiniones públicas.
- **Estrategias multidimensionales o híbridas**: Un tercer elemento característico del conflicto en la zona gris son las estrategias híbridas con empleo intencionado, multidimensional e integrado de diversos instrumentos de poder: políticos, económicos, sociales, informacionales, diplomáticos y también militares. Dichas estrategias tratan de aprovechar oportunidades y explotar vulnerabilidades del oponente en esos distintos ámbitos para ejercer coerción y/o degradar su proceso de toma de decisiones políticas con el fin de obtener ventaja competitiva sobre él. La peculiaridad de lo militar en estas estrategias es su carácter fundamentalmente simbólico con intención coercitiva, utilizándose para señalar, intimidar u obtener ventaja en la escalada, y excepcionalmente para respaldar a terceros actores que sí recurren a la fuerza –y en ocasiones a gran escala– en el marco de una guerra por delegación (*proxy war*), en una diada de conflicto diferente a aquella en la que se está desarrollando el conflicto en la zona gris. Lo característico por tanto del conflicto en la zona gris es el empleo mayoritario e integrado de herramientas no militares.

Las estrategias híbridas con empleo intencionado, multidimensional e integrado de diversos instrumentos de poder, tratan de aprovechar oportunidades y explotar vulnerabilidades del oponente.

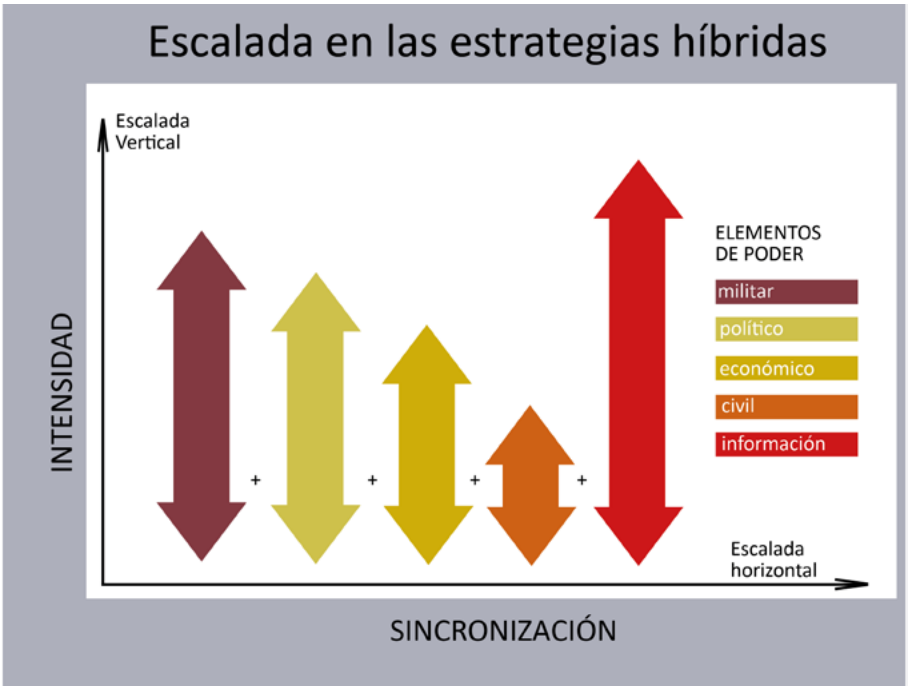


Gráfico1: Escalada en las estrategias híbridas. Elaborado por el DSN
Fuente original: Multinational Capability Development Campaign (MCDC) (2019), Countering Hybrid Warfare, MCDC Countering Hybrid Warfare Project. p. 14.

Dentro del repertorio de estrategias híbridas hay dos que afectan particularmente a la desinformación:

- **Respaldo a actores políticos antisistema** en la política interna del rival para perturbar sus procesos de toma de decisiones y obtener ventaja competitiva sobre él. Además de mediante apoyo mediático y operaciones de influencia que se comentan en el siguiente punto, la ayuda a esos actores puede realizarse mediante canales directos e indirectos con el propósito de agudizar divisiones preexistentes y erosionar la legitimidad de las instituciones políticas del Estado oponente. Resulta obvio que en circunstancias normales la multiplicidad de actores y la complejidad de los problemas dificultan la labor de gobierno democrático tanto a nivel estatal como supranacional, por ejemplo, en la Unión Europea o la Alianza Atlántica. Al mismo tiempo, la consabida urgencia del presente –con ciclos de información ininterrumpidos durante las 24 horas del día–,

unida al cortoplacismo marcado por el calendario electoral lleva a descuidar la planificación y el compromiso a largo plazo.

Estas circunstancias favorecen las acciones de zona gris destinadas a provocar disfunciones en los procesos de decisión política rivales. Más aún si el Estado objetivo presenta vulnerabilidades en términos de corrupción, instituciones débiles, fracturas sociales graves y polarización política. La ventaja es todavía mayor cuando el actor que opta por el conflicto en la zona gris posee un proceso de toma de decisiones menos transparente e institucionalizado –sin los controles y contrapesos propios de los sistemas democráticos– que le permitan desarrollar campañas de injerencia exterior clandestinas sin dar explicaciones a su propia opinión pública.

- **Operaciones de influencia sobre la opinión pública** internacional y sobre la opinión pública del adversario, construyendo y difundiendo meta-narrativas –en lo posible de manera encubierta, a través de terceros– que afecten a los procesos políticos de otros Estados, favoreciendo los intereses de quien las promueve y deslegitimando las instituciones del bando rival. Es una línea de acción estratégica estrechamente vinculada a la anterior. Dichos meta-relatos se difunden en el espacio público mediante informaciones sesgadas o falsas y dirigidas a audiencias objetivo, favorables a esos puntos de vista. Es frecuente el recurso a teorías de conspiración. Este empeño puede verse amplificado en las redes sociales por la sinergia con otros individuos y grupos que compartan un adversario común o una causa semejante.

  Las circunstancias del presente y las tendencias futuras ofrecen nuevas oportunidades en comparación con conflictos pretéritos en la zona gris, como la Guerra Fría donde Estados Unidos y la Unión Soviética hicieron amplio uso de las operaciones de influencia. La pluralidad de los canales de difusión, el uso generalizado de las redes sociales, combinado con adelantos en inteligencia artificial, incrementa sustancialmente el alcance de dichas operaciones El empoderamiento de grupos e individuos, que gracias a la tecnología pueden coordinarse y actuar de manera efectiva y barata, también multiplica los efectos. Esta faceta del cambio social y político posee numerosos aspectos positivos, y a la vez crea oportunidades a las estrategias propias de la zona gris.

Guerra informativa

Hoy en día, el concepto de guerra informativa se emplea – junto con la desinformación o la guerra híbrida – para definir todas aquellas actividades relacionadas con el uso y explotación del entorno online realizadas para proyectar la influencia política bajo el umbral del conflicto armado. Aunque esta parece ser la concepción que se ha consolidado entre la opinión pública, la guerra y/o las operaciones informativas ni son un fenómeno nuevo, ni se circunscriben al mundo virtual, ni se limitan a la propaganda, la desinformación, la manipulación, las noticias falsas o ciberataques. De hecho, la información siempre ha sido un activo estratégico tanto en tiempo de paz como en periodos de guerra. Al igual que muchos otros países, Estados Unidos considera que la información es una de las tradicionales herramientas del poder nacional junto con la diplomacia, la economía o la defensa. Estos instrumentos pueden implementarse tanto mediante un enfoque gubernamental liderado por la Casa Blanca para coordinar la proyección del poder nacional, como en el marco de un enfoque integral en el que colaboren otros actores para responder a crisis internacionales.

La información siempre ha sido un activo estratégico tanto en tiempo de paz como en periodos de guerra.

En consecuencia, una amplia gama de agencias y departamentos del país participan en actividades de comunicación estratégica, diplomacia pública, detección de operaciones de influencia extranjeras. Sin embargo, ninguno de estos actores realiza operaciones de información (*information operations*) propiamente dichas, ya que éstas – vinculadas tradicionalmente con la propaganda, las operaciones psicológicas, los asuntos públicos o la guerra electrónica – son formalmente consideradas como una función militar bajo la responsabilidad del Departamento de Defensa.

En este sentido, el entorno informativo donde tienen lugar estas actividades se considera como un espacio que «…integra numerosos atributos sociales, culturales, cognitivos, técnicos y físicos que afectan al conocimiento, comprensión, creencias, opiniones, cosmovisiones y, en última instancia, a las acciones de un individuo, grupo, sistema, comunidad u organización. El espacio informativo, que también incluye los sistemas técnicos y sus datos, afecta y se extiende a todo el entorno operativo.»

Este se compone de tres dimensiones interrelacionadas:

- **Física:** los sistemas de mando y control, los actores clave en la toma de decisiones y las infraestructuras necesarias para actuar en este entorno.
- **Informativa:** dónde y cómo se recolecta, procesa, almacena, disemina o protege la información.
- **Cognitiva:** las mentes de aquellos que transmiten reciben, responden o interactúan con la información.

Este entorno que aúna elementos físicos, lógicos y psicológicos constituiría el campo de batalla de la guerra informativa. Su ejecución podrá requerir el uso de una amplia gama de herramientas, entre las cuales destacan:

- **Ciberoperaciones:** cualquier actividad de tipo defensivo, ofensivo o de explotación – para obtener inteligencia mediante la explotación de los datos obtenidos de las redes y sistemas de información adversarios – realizada en el ciberespacio en apoyo a las operaciones informativas.
- **Operaciones de apoyo a la información militar:** herederas de las operaciones psicológicas, estas actividades se realizan en la dimensión cognitiva para influir sobre las emociones, motivaciones, razonamientos o comportamientos de individuos, grupos sociales, organizaciones o gobiernos adversarios, aliados y neutrales.
- **Guerra electrónica:** actividades realizadas en el espacio electromagnético (desde la interferencia de las comunicaciones radioeléctricas a la suplantación o *spoofing* de la señal de GPS) para degradar las capacidades informativas del adversario.
- **Seguridad de las operaciones:** fundamentada en la identificación y protección de toda la información sensible vinculada con las unidades o las operaciones que pueda ser explotada por la inteligencia adversaria. Tal y como se ha observado en numerosas ocasiones, la exposición del personal militar a los servicios de mensajería online, aplicaciones móviles, sistemas de geolocalización o a las redes sociales virtuales hace que la seguridad de las operaciones sea el puntal de cualquier actividad militar.
- **Engaño (decepción en el léxico militar español):** mediante una amplia gama de actividades – siendo la desinformación una de ellas – para confundir al adversario sobre las capacidades, intenciones u operaciones propias y así lograr que tome decisiones o realice

acciones que, siendo contrarias a sus intereses, contribuyan al logro de los objetivos propios.

Por su parte, la concepción rusa plantea una visión integrada, centrada en manipular las mentes de la sociedad y empleada en tiempo de paz, zona gris y guerra. El régimen ruso considera que puede proyectar su poder mediante una amplia gama de vectores, desde la diplomacia o la economía hasta la cultura, la moral, el arte o el medioambiente. Combinados, éstos pueden emplearse como arma política para alterar la correlación de fuerzas, coartar las acciones del adversario controlando la escalada, subvertir moralmente y desestabilizar políticamente su sociedad o apoyar el logro de los objetivos estratégicos sin apenas utilizar la fuerza armada.

En el epicentro de este enfoque se halla la información, considerada por el Kremlin como la principal herramienta para proyectar el poder nacional, uno de los fundamentos de la soberanía nacional y – en línea con la tradición soviética – uno de los principales activos a salvaguardar para mantener la estabilidad política, social, moral y espiritual del país frente a influencias externas. Esta concepción que prima la protección del espacio informativo nacional y la proyección de la influencia exterior es anterior a la llegada de internet. Sin embargo, fue en la década de 1990 cuando la comunidad de inteligencia rusa alertó de que las nuevas tecnologías eran una amenaza a la seguridad nacional por su potencial desestabilizador.

Asumiendo que el entorno informativo comprende todo aquello que pueda relacionarse directa o indirectamente con la información (desde los medios de comunicación o el espacio radioeléctrico y cibernético hasta la percepción que se tiene del país dentro y fuera de sus fronteras o la moral de su población), el régimen ruso entiende que éste se compone de dos dimensiones: una informativo-técnica y otra informativo-psicológica. Temiendo que un adversario pueda atacar ambas dimensiones (la informativo-técnica para destruir, por ejemplo, el sistema de mando y control militar y así degradar su disuasión nuclear, y la informativo-psicológica para desmoralizar a la población o deslegitimar el gobierno), es esencial que Moscú logre su seguridad informativa.

Este conjunto de factores ha condicionado el desarrollo de la guerra informativa rusa, «…un conflicto entre dos o más estados en el espacio informativo con la finalidad de dañar los sistemas, procesos, recursos o estructuras informativas, erosionar los sistemas políticos, económicos y sociales, llevar a cabo campañas psicológicas masivas contra la población del estado para desestabilizar la sociedad y el gobierno o forzar al estado para que tome decisiones en el interés de sus oponentes.» (Colom-Piella, 2020)

Considerada por muchos estrategas del país como el componente de una confrontación informativa global en la que Occidente quiere imponer su voluntad sin recurrir al enfrentamiento militar directo, la guerra informativa va mucho más allá de la desinformación, las noticias falsas o los ciberataques.

Moscú entiende que la guerra informativa puede servir tanto para alcanzar los objetivos políticos sin necesidad de emplear la fuerza armada mediante el empleo de una amplia gama de actividades no-militares en los dominios físico, lógico y cognitivo para negar, sabotear o manipular la información, como para contribuir a la conducción – modelando la opinión pública, apoyando a las unidades terrestres, navales o aéreas o batiendo objetivos informativos – de las operaciones militares. Susceptible de utilizarse en tiempo de paz, escalada y conflicto abierto en los niveles estratégico, operacional y táctico, la guerra informativa posee una vertiente ofensiva, enfocada al logro de la superioridad informativa sobre el adversario, y defensiva, para garantizar la seguridad informativa del país y así contribuir a la estabilidad estratégica.

Moscú entiende que la guerra informativa puede servir para alcanzar los objetivos políticos sin necesidad de emplear la fuerza armada mediante el empleo de una amplia gama de actividades.

Además, entendiendo que el entorno informativo comprende todo lo relacionado con la información y que cualquier soporte, canal, medio o vector físico, radioeléctrico, digital o cognitivo puede ser destruido, degradado, alterado o corrompido, cualquier tecnología, medio o actividad que posea una dimensión informativa puede convertirse en un arma informativa. En consecuencia, la paralización de un sistema de defensa aérea, la destrucción de una estación de comunicaciones, la suplantación de una señal de GPS, la interferencia de las transmisiones de radiotelevisión, la denegación de un servicio web, la exfiltración de información personal, la eliminación de un periodista, una declaración oficial, una cadena de bulos difundida en plataformas de mensajería o una imagen alterada digitalmente y transmitida por una red social son algunas de las armas que pueden utilizarse para combatir en el espectro informativo. Combinadas, éstas se orientarán al logro de efectos informativo-técnicos sobre las infraestructuras y sistemas enemigos e informativo-psicológicos sobre sus percepciones.

En conclusión, Moscú concibe la guerra informativa como una actividad integral que, susceptible de emplearse en todo el espectro del conflicto, requiere la participación de una amplia gama de actores y de medios. En consecuencia, no debería asombrarnos que servicios secretos, fuerzas armadas y medios

de comunicación colaboren con *hacktivistas* nacionalistas, ejércitos de *trolls* o grupos de *hackers* organizados. Aunque el centro de gravedad de esta contienda son las mentes de los ciudadanos, las campañas rusas en Ucrania y Siria han vuelto a recordar que la guerra informativa no sólo permite proyectar el poder dificultando la atribución de las acciones, sino que también sirve para apoyar la conducción de operaciones militares. Solamente si dejamos de recurrir a grandes conceptos cada vez más vacíos de contenido y estudiamos con detalle la doctrina soviética y rusa podremos comprender que la guerra informativa es un continuo que no se limita a la zona gris del conflicto, que va mucho más allá que la desinformación o las noticias falsas y que puede ser un componente de una guerra política de alcance mucho mayor.

La guerra informativa es un continuo que no se limita a la zona gris del conflicto, que va mucho más allá que la desinformación o las noticias falsas y que puede ser un componente de una guerra política de alcance mucho mayor.

RELEVANCIA DE DEFINIR EL FENÓMENO DE LA DESINFORMACIÓN Y SU ADECUACIÓN AL PROTOCOLO DEL DSN

La desinformación, definida como «información verificablemente falsa o engañosa creada, presentada y difundida con fines de lucro económico o engaño intencionado al público» (Comisión Europea, 2019), se ha convertido en un problema clave para las sociedades democráticas contemporáneas. Este elemento, su carácter deliberado, es la diferencia de lo que en el mundo anglosajón se define como *misinformation*, que se refiere a la difusión no-intencionada de información falsa o no veraz por parte de los usuarios. Para la Comisión Europea, la desinformación, por el contrario, requiere, además de la inautenticidad, la coordinación y la ocultación de los actores, sus actividades y propósitos, con un propósito deliberado y dañino.

La desinformación es difícil de detectar, pero sus consecuencias son evidentes.

Es un fenómeno que, pese a su naturaleza basada en el enmascaramiento, el disimulo y la ocultación, ha cobrado gran protagonismo en el debate público. La desinformación es difícil de detectar, pero sus consecuencias son evidentes.

El uso de la mentira como recurso de manipulación deliberada de la ciudadanía y como medio para perjudicar al rival es tan antiguo como la humanidad misma. Sin embargo, durante el siglo XX, primero con el auge de los totalitarismos y las guerras mundiales, y, más tarde, con la Guerra Fría que enfrentó soterradamente a los bloques mundiales, la propaganda y la desinformación se convirtieron definitivamente en un mecanismo empleado masivamente por las potencias en conflicto (Bittman y Godson, 1985; Bittman, 1990; Snyder, 1997). La diseminación planificada de mensajes falsos, con el objetivo de perjudicar al rival, al tiempo que se reforzaba la cohesión de los propios, se convirtió en una práctica esencial en la geoestrategia de las potencias mundiales.

Desde el comienzo del siglo XXI, la globalización de la comunicación propiciada por internet y, en particular, por el auge de las redes sociales, ha reconfigurado de manera radical los procesos y canales de la comunicación pública. Con ello, también ha transformado el modo en el que se disemina internacionalmente la desinformación. Los medios periodísticos han perdido buena parte de su rol

como intermediarios y garantes de la calidad informativa. En su lugar, las plataformas digitales se han erigido en canales principales de distribución instantánea y ubicua de todo tipo de contenidos, incluidos los falsificados. En este nuevo escenario global de la comunicación, necesitado de mayor regulación o escrutinio a través de un código de buenas prácticas reforzado, como así propone la Comisión Europea, los diseminadores de contenidos adulterados han encontrado un entorno ideal para sus propósitos.

Foto 2: Vigilia por las 298 víctimas mortales del vuelo MH17, en Petaling Jaya, Malasia, en 2014. EFE/Azhar Rahim

Numerosos casos confirman, en efecto, el incremento en los últimos años de los episodios de desinformación en el marco de conflictos bélicos, pugnas geoestratégicas, y procesos políticos y sociales y, por supuesto, en torno a la pandemia de la COVID-19 (Salaverría-Aliaga, 2021). Entre los ejemplos más reseñables está la desinformación en torno al enfrentamiento entre Rusia y Ucrania. En el marco de ese conflicto, que resultó en la ocupación y posterior adhesión del territorio ucraniano de Crimea por parte de Rusia, se detectaron

diversos casos de desinformación. El más destacado tuvo lugar en julio de 2014, con motivo del derribo por un misil tierra-aire del vuelo comercial MH17, entre Ámsterdam y Kuala Lumpur, que se saldó con la muerte de 283 pasajeros y 15 miembros de la tripulación; la determinación de la autoría de ese acto produjo una espiral de desinformación que ha sido analizada en varios estudios (Khaldarova y Pantti, 2016; Rietjens, 2019).

Al año siguiente, en 2015, comenzó la carrera electoral de Donald J. Trump hacia la presidencia de Estados Unidos, que terminó con su victoria contra pronóstico en las elecciones de noviembre de 2016. Diversos estudios han explicado este inesperado triunfo de Trump como resultado, entre otros factores, de su uso estratégico de la desinformación (Swire et al., 2017). Posteriormente, estas prácticas desinformativas continuaron durante su mandato. De acuerdo con una investigación de Washington Post, Trump acumuló durante sus cuatro años de presidencia más de 30.000 afirmaciones falsas, exageraciones y mentiras (Kessler et al., 2021).

Las evidencias sobre campañas de desinformación también han aparecido en otros procesos políticos relevantes de los últimos años. Por ejemplo, en 2016 con motivo del referéndum en el Reino Unido (Bastos y Mercea, 2019), en las elecciones presidenciales de Francia de 2017 (Ferrara, 2017), o durante las elecciones generales de Brasil de 2018, en las que resultó elegido Jair Bolsonaro (Recuero et al., 2020). En España, el proceso independentista en Cataluña también ha sido un caso especialmente fecundo en mensajes desinformativos (Aparici et al., 2019), con sospechas de injerencias por parte de países extranjeros, particularmente de Rusia (Schwirtz y Bautista, 2021).

Al margen de la política, con motivo de la pandemia de la COVID-19, se han identificado asimismo abundantes casos de desinformación pública con distintas tipologías (Salaverría et al., 2020) y protagonizadas por múltiples actores, incluidos los propios políticos de distintos países (Ricard y Medeiros, 2020). Entre esas campañas de desinformación en torno a la pandemia cabe destacar, en particular, las promovidas por movimientos negacionistas y por grupos activistas antivacunas (Germani y Biller-Andorno, 2021; Loomba et al., 2021).

Estos ejemplos demuestran que, hoy día, buena parte de las campañas de desinformación afectan a la seguridad de los países. Existen también operaciones desinformativas de una incidencia más limitada, como las orquestadas, por ejemplo, para propiciar estafas económicas o para tratar de socavar el debate democrático, exacerbar la polarización social o interferir en la integridad de los procesos electorales. También hay campañas orientadas

a crear artificialmente climas de opinión y promover la confrontación social, con mensajes falsos que con frecuencia se vinculan a los discursos de odio. Tanto si se trata de campañas de largo alcance, impulsadas artificialmente con procedimientos sofisticados tales como las redes de *bots*, como si son episodios más aislados o de menor trascendencia e intensidad, la desinformación produce desestabilización, desconfianza y preocupación en la ciudadanía. Por eso debe ser enfrentada como un problema social relevante.

Hoy día, buena parte de las campañas de desinformación afectan a la seguridad de los países.

Enfrentar este problema social y de seguridad comienza por una precisa delimitación del concepto de desinformación. Como han puesto de manifiesto múltiples estudios, los fenómenos vinculados a la desinformación son muy variados. Esto ha alumbrado un conjunto de términos altamente polisémicos y, con frecuencia, equívocos (Galdón, 1994; Magallón, 2019). En concreto, en los últimos años se ha popularizado la cuestionada expresión de noticias falsas o *fake news* (Tandoc Jr et al., 2018, 2021). Sin embargo, este es un concepto cuestionado por los investigadores y las instituciones públicas. En sus informes y documentos recientes en torno a la desinformación, la Comisión Europea emplea los términos *disinformation* y *misinformation* para designar este fenómeno, pues resultan conceptualmente más precisos y menos sesgados a la hora de identificar las distintas modalidades de falsedades comunicadas públicamente.

DESINFORMACIÓN EN EL ÁMBITO DE UNA INJERENCIA DE UNA POTENCIA EXTRANJERA

La desinformación se ha convertido en una grave amenaza a la viabilidad de los sistemas democráticos. La propagación de manera deliberada de información falsa, sesgada o manipulada con un propósito hostil tiene la capacidad de erosionar los cimientos sobre los cuales se asientan las sociedades abiertas. La desinformación apunta hacia uno de los requisitos básicos del orden político liberal: la superioridad de los hechos sobre las emociones. Pero lo hace de una manera lenta y sutil, lo cual le confiere una peligrosidad mucho mayor que cualquier ataque frontal, ya que dificulta que la sociedad pueda reaccionar. Cuando la autoridad de los datos se erosiona, las emociones llenan el vacío. Aunque estas campañas pueden tener objetivos específicos en el corto plazo, en última instancia generan un efecto permanente al dañar la "trinidad de la confianza" (Ingram, 2020): confianza en los demás, confianza en la autoridad/experiencia y confianza en la democracia. Cuanto más se deterioran estas bases, más proclive es una sociedad a legitimar formas de gobierno no democráticas e incluso a implicarse en un activismo político de carácter violento.

La desinformación apunta hacia uno de los requisitos básicos del orden político liberal: la superioridad de los hechos sobre las emociones.

Las campañas de desinformación no son únicamente el fruto de la acción espontánea de un grupo de políticos y creadores de opinión sin escrúpulos, sino que históricamente han sido el resultado de la acción metódica de grandes burocracias (Rid, 2020). La desinformación era, y en muchos sentidos sigue siendo, el dominio de los organismos de inteligencia -dirigidos profesionalmente, mejorados continuamente, y generalmente empleados contra adversarios extranjeros. Sin embargo, las heridas más destructivas para la causa democrática han sido autoinfligidas. En los últimos años se ha producido una convergencia (Sipher, 2018) entre actores externos e internos, estatales y no estatales. Uno de los principales desafíos a la democracia es precisamente que tiene que hacer frente a la acción hostil de grupos distintos que hacen las mismas cosas por razones diferentes, dándose con ello una unidad de intereses entre actores que parten de puntos de partida distintos.

Aunque pueda mantener diferentes posturas fundamentadas sobre la magnitud e intensidad del cambio que las nuevas tecnologías han aportado a estas acciones de manipulación, lo cierto es que la historia de la propaganda

nunca ha sido una progresión lineal (Jowett y O'Donnell, 2006). En todos los casos, aquellos que han tratado de manejar o controlar a otros han hecho un amplio e inteligente uso de las formas de comunicación de las que disponían. El medio de distribución no sólo ha sido una herramienta, sino un vector que transformaba el propio contenido del mensaje y sus objetivos. Se ha prestado mucha atención a la forma en la cual está construido el mensaje para tratar de explicar por qué unos manipuladores tienen éxito y otros no, sin embargo, se ha minusvalorado el hecho de que la gente construye diferentes significados acordes a su experiencia como lector, oyente, espectador o internauta.

En la era digital, cuando la gente publica, comenta, comparte y busca, está participando en el proceso de la información de una manera absolutamente inédita. Somos actores en nuestro propio consumo de información, y esto representa un cambio sutil, pero muy importante. La participación es un tipo de inversión cognitiva. Las personas se comprometen de manera diferente cuando son ellas mismas quienes participan en el relato, el cual termina siendo parte de su propia experiencia.

La investigación sobre las operaciones de influencia nos muestra que estas operaciones rara vez tratan de cambiar lo que la gente piensa. Se trata más bien de confirmar lo que la gente ya cree o de diseminar narrativas que siembren dudas sobre la veracidad o autenticidad de los hechos. Ahí reside el gran peligro de la desinformación: lejos de aportar datos que incomoden y hagan que el receptor tenga que asumir el esfuerzo de replantearse aquellas de sus opiniones que chocan con la realidad, la desinformación arroja a su consumidor a un confortable estado de confirmación de sus prejuicios. Este efecto es especialmente gratificante cuando la desinformación respalda posiciones que el individuo se muestra reticente a defender de manera abierta, porque considera que son impopulares y le pueden acarrear el reproche de los que le rodean.

La desinformación necesita alimentar la polarización en la sociedad, porque cuando se desprenden los matices de cualquier cuestión resulta inevitable que la gente deba posicionarse en términos binarios: a favor o en contra.

Este modelo de «propaganda participativa» (Rogers et al., 2019) implica inundar a las personas con sesgos de confirmación, y privarlas de oportunidades para cuestionar y dudar de otras visiones alternativas. La desinformación necesita alimentar la polarización en la sociedad, porque cuando se desprenden los matices de cualquier cuestión resulta inevitable que la gente deba posicionarse en términos binarios: a favor o en contra. La desinformación no tiene la capacidad para crear nuevas brechas dentro de la sociedad, pero sí para extender y radicalizar las ya existentes (Robinson et al., 2018).

Internet ha dado un nuevo impulso a las operaciones de desinformación debido a los siguientes factores

Ha disminuido radicalmente en coste en términos de tiempo, dinero y esfuerzo, y con ello, ha ampliado el número de actores que participan en el juego de la desinformación. La puesta en marcha de una campaña que alcance a millones de destinatarios ha dejado de ser una capacidad exclusiva de aquellos que controlan o tienen acceso al entramado de los grandes medios de comunicación. El coste de empleo de estos recursos es tan reducido que sus impulsores, en ocasiones, ni siquiera pretenden convencer o persuadir, sino simplemente abrumar (Manjoo, 2017). Producir y distribuir desinformación cada vez es más fácil, lo que explica el desinterés por las operaciones de extrema sofisticación, donde se individualiza el contenido y se actúa de manera prolongada sobre una misma audiencia. Por el contrario, ha predominado el enfoque del mínimo esfuerzo. Cuando se persiguen objetivos tan genéricos como como agravar las fracturas sociales, provocar desconfianza o indignación, el error es fácilmente asumible, ya que este apenas genera un perjuicio para el instigador de estos mensajes. El ciberespacio ofrece un amplio margen para la acción encubierta y esto disminuye enormemente el riesgo reputacional para los manipuladores.

El ciberespacio ofrece un amplio margen para la acción encubierta y esto disminuye enormemente el riesgo reputacional para los manipuladores.

Ha erosionado el papel de los medios de comunicación como mecanismos de autentificación. Con carácter previo a la aparición de internet, los medios tradicionales ejercían la labor de mediadores, sirviendo estos como mecanismo de filtrado de la autenticidad y relevancia de las informaciones que alcanzaban a la opinión pública. La irrupción de internet no sólo ha abierto una vía directa de comunicación de entre los que crean los mensajes y quienes lo consumen, sino que ha forzado a los medios tradicionales a alimentarse directamente de este nuevo escenario. Las informaciones que circulan originalmente en internet tienen capacidad por sí mismas para convertirse en noticias de amplio alcance, sin que medien aquellos que poco tiempo atrás monopolizaban la decisión sobre qué noticia es digna de ser conocida por la opinión pública. Internet no solo ha arrebatado la centralidad a los medios tradicionales, sino que añadió una crisis en el modelo de negocio de este sector, el cual no fue capaz de adaptarse con agilidad a la pérdida de ingresos publicitarios. Las empresas empezaron a descapitalizar sus plantillas y optar por nutrirse de informaciones cuya consecución no fuese especialmente onerosa. Los

medios no sólo perdieron su propia capacidad para detectar y neutralizar la desinformación que llegaba a sus redacciones, sino que se convirtieron en víctimas especialmente vulnerables a estas manipulaciones, porque la desinformación es gratuita y además genera audiencia.

La desinformación no sólo fluye al margen de los medios tradicionales, sino que su contenido también apunta contra ellos. En buena parte de estos contenidos subyace el meta-relato de que los medios tradicionales son una mera extensión de *establishment* político-económico (Badillo, 2019), estas corporaciones no sólo tendrían como principal misión construir una narrativa que beneficie los intereses de sus poderosos propietarios, sino también silenciar y desacreditar aquellas informaciones que cuestionan o contradice esta estructura de intereses. Que la información que circula en los "medios alternativos" de internet no encuentre eco en los medios de comunicación tradicionales, es percibido como una prueba adicional de su verosimilitud por parte de una audiencia instalada en una visión conspirativa de la realidad. La desinformación vive en una especie de profecía autocumplida: cuanto más marginal es su difusión, más creíble resulta.

La desinformación vive en una especie de profecía autocumplida: cuanto más marginal es su difusión, más creíble resulta.

POR QUÉ NO SON "NOTICIAS FALSAS" *(FAKE NEWS)*

Antes de abordar la definición de desinformación conviene detenerse en otro concepto que se ha utilizado en muchas ocasiones como sinónimo: el de *fake news*. El Diccionario Merriam-Webster rastrea el origen de este término en la historia de la lengua inglesa y detecta que se empieza a utilizar a finales del siglo XIX. Sin embargo, su uso no se extiende de forma masiva hasta 2016, tras el referéndum del *Brexit* en el Reino Unido y la victoria de Donald Trump en las elecciones estadounidenses (Merriam-Webster, 2018). Su expansión a partir de acontecimientos políticos es una característica que marca el uso de *fake news* y, de alguna manera, también lo contamina. Esta popularización del término hace que también aumente el interés del mundo académico por él y que se multiplique el número de estudios que tratan de delimitar a qué nos referimos cuando hablamos de *fake news*.

Uno de los principales obstáculos que se encuentran estas investigaciones es que no todo el mundo entiende lo mismo por *fake news*. El Reuters Institute de la Universidad de Oxford (Newman et al., 2017), señalaba que, a la hora de encuestar al público, habían detectado tres interpretaciones diferentes de este término: noticias "inventadas" para ganar dinero o desacreditar a otros; noticias que tienen una base en hechos, pero se han "modificado" para adaptarse a una agenda en particular y noticias con las que la gente no se siente cómoda o no está de acuerdo.

También (Quandt et al., 2019) destacan la polisemia de *fake news* y la confusión que puede generar. Para ellos, por un lado, puede entenderse como las «noticias fabricadas que circulan a través de las redes sociales». Pero también funciona como una expresión diseñada para desacreditar a los medios de comunicación tradicionales. En este escenario, habitualmente los académicos trabajan con la primera definición, pero los políticos tienden a utilizarlo con más frecuencia en la segunda, como arma arrojadiza contra la prensa que no les gusta. Este doble uso hace que al público no le quede claro de qué se habla cuando se habla de *fake news*.

Fake news es un concepto que los políticos tienden a utilizarlo como arma arrojadiza contra la prensa que no les gusta.

Pero, más allá del uso político del término, dentro del mundo académico también hay distintas aproximaciones a la definición de *fake news*. Algunos investigadores se centran en el aspecto formal y destacan en sus definiciones el intento de imitar a las noticias de los medios convencionales. El filósofo Gelfert (2018) sostiene que *fake news* «debe reservarse para casos de presentación deliberada de afirmaciones (típicamente) falsas o engañosas como noticias, cuando sean engañosas por diseño». La también filósofa Rini (2017) hace hincapié en que se trata de contenidos que habitualmente imitan «las convenciones del reportaje de los medios tradicionales, sin embargo, sus creadores saben que son significativamente falsos, y se difunden con los dos objetivos de ser ampliamente transmitida y de engañar al menos a parte de su audiencia». Por su parte, Lazer et al. (2018) se centran en que las *fake news* imitan el contenido de los medios sólo «en la forma, pero no en el proceso organizativo o en la intención».

Allcott y Gentzkow (2017) ponen el foco en la reacción del público y definen *fake news* como «artículos de noticias que son intencional y verificablemente falsos y podría inducir a error a los lectores». Aclaran que ellos reservan ese concepto para contenidos con implicaciones políticas. Descartan los errores periodísticos, los rumores que no se generan a raíz de un artículo, los reportajes partidistas, las teorías de la conspiración o las sátiras que es poco probable que engañen al público. Sin embargo, Molina et al. (2018) sí dan mucha importancia a la vertiente humorística. Recuerdan que la expresión *fake news* se usaba antes de los acontecimientos políticos de 2016 vinculada a programas o publicaciones satíricas como The Daily Show o The Onion. Esta tradición la tienen en cuenta cuando definen *fake news* como «contenidos que parecen ser noticias, difundidas en el Internet o utilizando otros medios, generalmente creados para influir en las opiniones políticas o como una broma».

Klein y Wueller (2017) tratan de delimitar el concepto para usarlo en el ámbito legal. Por eso renuncian a incluir el humor, que consideran protegido por la libertad de expresión, y definen *fake news* como «la publicación en línea de exposiciones de hechos que son falsos intencionalmente y a sabiendas». Pero reconocen que el término arrastra connotaciones ideológicas porque los políticos lo utilizan para describir los reportajes de medios tradicionales que no les gustan.

Esta diversidad de enfoques la recogen Tandoc et al. (2018), que revisan los artículos académicos que usaron ese término entre 2003 y 2017 y comprueban que, en ese espacio de tiempo, se ha usado *fake news* para referirse a

fenómenos muy diferentes como la sátira, la parodia, la imitación de noticias, la manipulación de fotografías, la publicidad o la propaganda.

En definitiva, *fake news* es un concepto ambiguo y difícil de acotar sobre el que no se ha alcanzado una definición de consenso en el mundo académico. Además, como señala Mayoral et al. (2019), *fake news* «constituye un oxímoron inaceptable. Si es falso, no es noticia. Y si es noticia (y por tanto ha habido verificación de contenidos), no es falso».

Fake news es un concepto ambiguo y difícil de acotar sobre el que no se ha alcanzado una definición de consenso en el mundo académico.

Salaverría-Aliaga (2021) también lo desaconseja porque «comporta un marco mental que sitúa el problema en el ámbito de los medios periodísticos». Rodríguez (2019) coincide, y añade que el término *fake news* se queda corto y «no abarca todas las dimensiones de la desinformación», además, «el discurso político se ha apropiado del término para desacreditar la labor del periodista». Algo que, como señalan Nielsen y Graves (2017) hace que se acabe usando *fake news* para referirse a «cualquier información que los políticos y la gente en general no se cree».

Por eso, en el ámbito académico y en textos de organismos oficiales es habitual que se rechace explícitamente el uso de *fake news*. Lo hizo el Gobierno británico a raíz de un informe del Comité de Tecnología Digital, Cultura, Medios y Deporte de la Cámara de los Comunes de 2019. En su lugar optan por utilizar desinformación (*disinformation*) e información errónea (*misinformation*). La primera la definen como «la creación deliberada y el intercambio de información falsa y/o manipulada con la intención de embaucar y engañar al público, ya sea con el propósito de causar daño, o con fines políticos, personales o económicos». En el caso de la información errónea no hay intencionalidad, la información falsa se comparte, pero se hace de forma inadvertida.

Facebook en su informe «Operaciones de información y Facebook» (Weedon et al., 2017) apunta en una dirección parecida. Descarta usar *fake news* porque ha abusado de ese término sin que esté muy claro a qué se refiere exactamente. Se utiliza para calificar contenidos que van desde artículos incorrectos, artículos de opinión, parodias, engaños, rumores, memes o errores fácticos de figuras públicas. Por eso ellos también apuestan por usar desinformación e información errónea (*misinformation*).

Esta diferenciación es muy similar a la que hacen Wardle y Derakhshan (2017), en su informe para el Consejo de Europa. En lugar de *fake news* ellos se refieren a desórdenes informativos y los dividen en tres categorías: desinformación

(*disinformation*), información errónea (*misinformation*), e información maliciosa (*malinformation*). Para ellos el término desinformación se refiere a la «información falsa y creada deliberadamente para dañar a una persona, grupo social, organización o país». La información errónea es información falsa pero no creada con la intención de causar daño y la información maliciosa es real, pero se comparte con la intención de perjudicar a una persona, organización o país.

La desinformación se sitúa en el corazón del problema porque aúna la elaboración de una mentira y la intención de engañar. Pero definirla tampoco es sencillo. En su informe sobre desinformación y libertad de opinión y expresión, la ONU señala algunas de las dificultades que entraña. Por ejemplo, afirma que es prácticamente imposible trazar una línea clara entre los hechos y la falsedad y entre la ausencia y presencia de intención de causar daño. Además, las opiniones, creencias o formas de expresión como la parodia y la sátira son difíciles de calificar como verdaderas o falsas y en muchos casos entra en juego la libertad de expresión, que no está sujeta al límite interno de veracidad.

La literatura académica que ha abordado esta definición se centra en dos características: el contenido es falso y existe intención de engañar. Lo hacen Lewandowsky et al. (2013), que se refieren a desinformación como «información completamente falsa que se difunde con fines propagandísticos, pero que puede identificarse como falsa más adelante». También Olmo y Romero (2019) hablan de la «difusión intencionada de información no rigurosa que busca minar la confianza pública, distorsionar los hechos, transmitir una determinada forma de percibir la realidad y explotar vulnerabilidades con el objetivo de desestabilizar». Mientras que Bontcheva et al. (2020) inciden más en los efectos perjudiciales que pueda tener y definen desinformación como «el contenido falso o engañoso que puede causar daño específico, independientemente de las motivaciones, la conciencia o los comportamientos».

La literatura académica que ha abordado esta definición se centra en dos características: el contenido es falso y existe intención de engañar.

Esas propuestas de definición manejan elementos que se repiten en todos los intentos que se han hecho de delimitar el concepto de la desinformación. Pero, como ya hemos visto en el caso de las *fake news*, también es importante que las definiciones generen un cierto consenso en torno a ellas. Por eso, es especialmente relevante la definición del Grupo de Expertos de Alto Nivel de la Comisión Europea (2018).

Ellos, tras detallar los motivos por los que el término *fake news* no es adecuado para abordar el fenómeno, describen desinformación como «información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para inducir a error deliberadamente a la población, y que puede causar un perjuicio público». El daño público incluye amenazas a los procesos democráticos, así como a bienes públicos como la salud, el medio ambiente o la seguridad de los ciudadanos de la Unión. La desinformación no incluye errores involuntarios, sátira y parodia, o las noticias o comentarios claramente identificados como partidistas. Esta definición tiene especial valor porque es el fruto del análisis de 39 expertos de distintos ámbitos presidido por Madeleine de Cock Buning. Además, se ha convertido en la referencia que usan no sólo las instituciones europeas, por ejemplo, en la Comunicación «La lucha contra la desinformación en línea: Un enfoque europeo», instrumentos como el «Código de buenas prácticas en materia de desinformación» o el reciente «Plan de Acción para la Democracia Europea (EDAP)», sino también una parte importante del mundo académico para hablar de desinformación.

Diferentes fenómenos de desinformación

Durante el periodo de su trabajo, el Grupo se familiarizó con diversas definiciones y conceptos relacionados con desinformación, que se pueden encontrar en varios documentos de la Unión Europea y otras organizaciones internacionales. El documento más reciente en el tema, el mencionado Plan de Acción para la Democracia Europea (EDAP), va más allá del concepto de desinformación e identifica 4 fenómenos relacionados: la desinformación, la información engañosa (*misinformation*), operaciones de influencia de la información e interferencia externa en el espacio de la información.

- **La información engañosa** es la información con contenidos falsos o engañosos compartida sin intención de perjudicar, aunque sus efectos pueden ser nocivos, por ejemplo, cuando la gente comparte información falsa con amigos y familia, de buena fe.
- **La desinformación** la define siguiendo los pasos del Grupo de Expertos de Alto Nivel de la Comisión Europea que incide en que se trata de un contenido falso, difundido con intención de engañar para conseguir algún tipo de beneficio y que puede causar un perjuicio público.
- **Operación de influencia en la información** así se entiende los esfuerzos coordinados tanto de actores nacionales como extranjeros para influir en un público destinatario usando una serie de medios engañosos, como la supresión de fuentes de información independientes, unida a la desinformación.
- **Injerencia extranjera en el espacio de información** a menudo realizada como parte de una operación híbrida más amplia, pueden entenderse los esfuerzos coercitivos y engañosos para perturbar la libre formación y manifestación de la voluntad política de las personas por parte de un actor estatal extranjero o de sus agentes.

El documento subraya la importancia de distinguir entre diferentes fenómenos para permitir diseñar respuestas políticas adecuadas: Para cada uno de estos tipos de fenómeno y dependiendo del actor, el canal y el impacto, son necesarias diferentes respuestas políticas, de conformidad con los derechos fundamentales y las normas democráticas. La información engañosa, cuando no hay intención de engañar, causar un daño público o lograr un beneficio económico, puede abordarse esencialmente mediante la comunicación proactiva, ofreciendo información fiable y sensibilizando sobre la necesidad de evaluar de forma crítica el contenido y las fuentes. Para hacer frente a los

demás fenómenos, en los que hay una intención de causar daño, es necesaria una respuesta más contundente y las capacidades de respuesta tienen que desarrollarse de forma continua.

Sin embargo, la pregunta clave en cuando hay que elegir la respuesta adecuada a los incidentes de desinformación, es ¿cómo se puede distinguir y atribuir los incidentes a uno de estos fenómenos? En este contexto, los servicios de la Comisión y el Servicio de Acción Exterior de la Unión Europea (SEAE) colaboran con los Estados miembros, la sociedad civil y la industria para perfeccionar definiciones y metodologías comunes con el fin de abordar las distintas categorías de actividades de desinformación y operaciones de influencia. Durante el periodo de su trabajo, el Grupo ha mantenido varias reuniones con los expertos del Grupo de Trabajo sobre Comunicación Estratégica en el Este (East StratCom) del SEAE quienes han compartido sus experiencias y el pensamiento sobre los componentes básicos para el entendimiento común y terminología del tema.

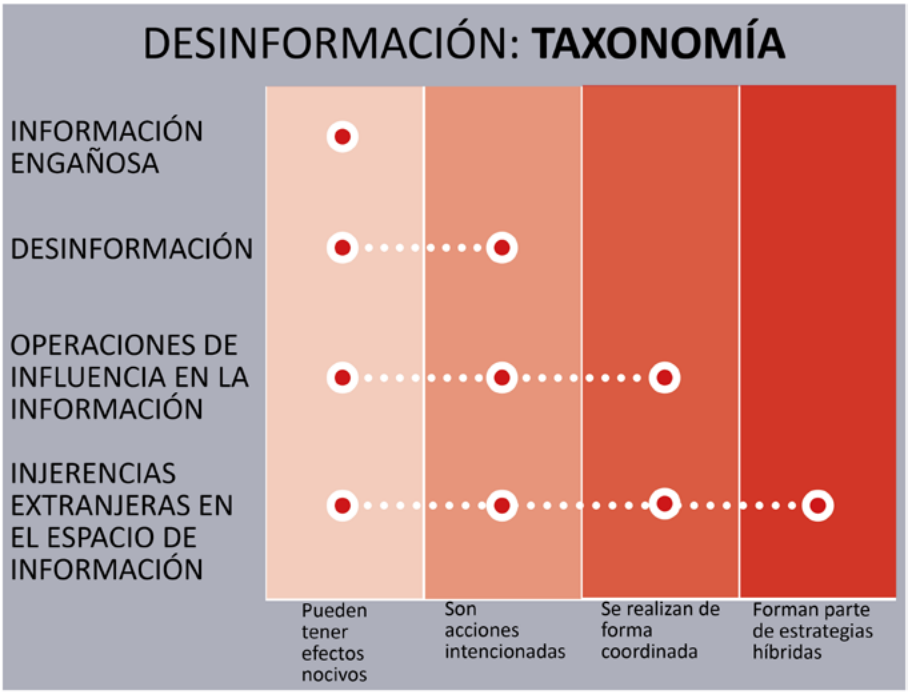


Gráfico 2: Fenómenos de la desinformación (taxonomía) según el Plan de Acción para la Democracia Europea
Elaborado por el DSN

DEFINICIÓN PROPUESTA

Teniendo en cuenta todo lo expuesto en el documento, el Grupo recomienda adoptar la definición del Grupo de Expertos de Alto Nivel de la Comisión Europea que considera desinformación «la información verificablemente falsa o engañosa que se crea presenta y divulga con fines lucrativos o para inducir a error deliberadamente a la población, y que puede causar un perjuicio público». Se trata de una definición fruto del trabajo conjunto de un grupo multidisciplinar, que abordó el problema de la desinformación desde todos los ángulos y alcanzó una conclusión que consideramos precisa, sólida y equilibrada.

Desde que se hizo pública en 2018, esta definición se ha convertido en una referencia internacional. Es la que utilizan la Unión Europea en sus documentos oficiales y también la han adoptado muchos otros organismos y administraciones públicas, ya sea de manera literal o asumiendo sus características fundamentales. Además, es la más habitual en los estudios académicos que investigan la desinformación y sus consecuencias.

También hay que tener en cuenta que, además de ser precisa, es importante que la definición resulte útil. Tanto la desinformación como las amenazas híbridas son fenómenos que superan las fronteras de un país. Se trata de desafíos globales y las acciones que se emprenden contra ellas se deben afrontar en coordinación con organismos internacionales. Por eso, nos parece acertado utilizar la definición que más consenso genera a nivel internacional, especialmente en el ámbito europeo. Hacerlo facilitará, por ejemplo, involucrarse en las actividades contra las injerencias extranjeras del Servicio Europeo de Acción Exterior de la Unión Europea.

No tendría sentido buscar definiciones alternativas que difícilmente mejorarían la del grupo de expertos de la Comisión Europea y, además, podrían entorpecer la coordinación en las acciones de lucha contra la desinformación más allá de las fronteras españolas.

BLOQUES PARA UN ENTENDIMIENTO COMÚN DE LOS DIFERENTES FENÓMENOS DE DESINFORMACIÓN

- **TTP:** Tácticas, Técnicas y Procedimientos de desinformación utilizados por los actores de amenazas. Según los expertos del SEAE, el análisis de tácticas, técnicas y procesos en los incidentes de desinformación, que utilizan los diferentes actores extranjeros (ej. relacionados con Rusia, China, Irán u otros países), son como los *fingerprints* específicos que ayudan a comprender, definir y atribuir los incidentes con un casi 80-90 por cientos de certitud.
- **Manipulación:** La actividad descrita como la desinformación e injerencia extranjera en el espacio de información es distinta de los patrones de comportamiento orgánicos y auténticos. La identificación y recogida de los TTP, es un elemento clave para establecer el criterio de manipulación; puede incluir varios elementos como la manipulación de hechos (por ejemplo, la difusión de información falsa / engañosa), el uso de cuentas de redes sociales falsas, la creación de sitios web falsos, cartas falsificadas, censura de voces críticas e independientes, acoso en línea, etc. Todas estas actividades manipulan el entorno de la información, dando una impresión distorsionada de la opinión pública y de la realidad.
- **Actividad de la zona gris:** mientras que el contenido terrorista y el discurso del odio, por ejemplo, se definen claramente como ilegales, desinformación e injerencia extranjera en espacio de información está utilizando deliberadamente la zona gris del espacio "no ilegal". Sin embargo, los incidentes de desinformación a veces pueden ocurrir en coordinación con un comportamiento ilegal.
- **Valores, procedimientos y procesos políticos:** la desinformación e injerencia extranjera en espacio de información tiene el potencial de afectar negativamente los derechos y libertades fundamentales, así como los valores en los que se ha fundado la Unión Europea, consagrados en el art. 2 del Tratado de la Unión Europea. Dichos bienes son la dignidad humana, la libertad, la democracia, la igualdad, el estado de derecho y

el respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías. Los bienes públicos se pueden desglosar aún más en consecuencia, como la protección de elecciones libres y justas, la libertad de expresión, etc. El nivel de amenaza puede determinarse con una evaluación de cómo, con qué finalidad y con qué intensidad se ven amenazados estos bienes.

- **Intención:** demostrar la intención de manipular el entorno de información es uno de los desafíos clave, pero también uno de los elementos clave para identificar la desinformación e injerencia extranjera. En este sentido, la combinación de diferentes TTP, así como su uso repetido por parte de un actor de amenazas, ayudará a establecer una intención de manipular el entorno de información.
- **Coordinación:** la desinformación e injerencia extranjera en el espacio de información tiene un cierto patrón de comportamiento y, por lo tanto, incluye un elemento de coordinación, es decir, la combinación de diferentes TTP para permitirles trabajar juntos de manera efectiva. También utiliza el ecosistema más amplio que ha evolucionado al incluir la capacidad de usar diferentes partes de este ecosistema. Por ejemplo, el uso de funcionarios gubernamentales junto con medios de comunicación patrocinados por el estado y organizaciones controladas por el estado.
- **Actores estatales o no estatales y / o sus "*proxies*":** La desinformación e interferencia extranjera puede ser llevada a cabo por gobiernos extranjeros o por actores extranjeros no estatales, incluidos los elementos que están directamente y públicamente vinculados, financiados y controlados por ellos. Sin embargo, esta actividad también puede incluir el uso de los llamados "*proxies*" o "representantes", donde no se establece un vínculo directo públicamente, pero donde dichos actores están vinculados, financiados y controlados de manera encubierta.

Los marcos analíticos y la metodología de la investigación de análisis

- **OpenCTI** es una plataforma de código abierto cofinanciada y desarrollada conjuntamente por la UE y Francia que permite a las organizaciones gestionar su conocimiento, información y datos de inteligencia sobre amenazas. Originalmente se creó para estructurar, almacenar, organizar y visualizar información técnica y no técnica sobre amenazas cibernéticas, pero también se ha demostrado que es aplicable a amenazas de desinformación e interferencia. OpenCTI permite a los usuarios fusionar información técnica (como TTP y observables) y no técnica (como atribución sugerida) mientras vincula cada pieza de información a su fuente principal (un informe, un artículo nuevo, etc.). (OpenCTI-Platform, 2022)
- **AMITT** (*Adversarial Misinformation and Influence Tactics and Techniques*) es un marco diseñado para describir y comprender los incidentes de desinformación. AMITT es parte del trabajo de adaptación de las prácticas de seguridad de la información (*infosec*) para ayudar a rastrear y contrarrestar la desinformación, y está diseñado para adaptarse a las prácticas y herramientas de seguridad de la información existentes. Los TTP existentes y conocidos se incluyen en el marco de forma continua. Las organizaciones pueden agregar sus propias TTP que sean relevantes para su trabajo. (COGSEC-Collaborative/Amitt, 2022)
- **STIX™** (*Structured Threat Information Expression)* es un formato de lenguaje y serialización que se utiliza para intercambiar inteligencia sobre amenazas cibernéticas (CTI). STIX es de código abierto y gratuito, lo que permite a los interesados contribuir. STIX permite intercambiar fácilmente información y datos sobre incidentes de desinformación en un formato estandarizado, lo que permite aún más la colaboración entre investigadores y analistas. (OASIS-Open, 2022)

REFERENCIAS BIBLIOGRÁFICAS

Allcott, H., Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, 31 (2): 211-36. https://doi.org/10.3886/E101177V1

Allen G. (2017) "Artificial Intelligence Will Make Forging Anything Entirely Too Easy", Wired June 30. https://www.wired.com/story/ai-will-make-forging-anything-entirely-too-easy/

Aparici, R., García-Marín, D., y Rincón-Manzano, L. (2019). Noticias falsas, bulos y trending topics. Anatomía y estrategias de la desinformación en el conflicto catalán. *Profesional de la Información*, 28(3): e280313. https://doi.org/10.3145/epi.2019.may.13

Badillo, A. (2019). *La sociedad de la desinformación: propaganda, «fake news» y la nueva geopolítica de la información*. Real Instituto Elcano. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/lengua+y+cultura/dt8-2019-badillo-sociedad-de-desinformacion-propaganda-fake-news-y-nueva-geopolitica-de-informacion

Bastos, M. y Mercea, D. (2019). The Botnet and User-Generated Hyperpartisan News. *Social Science Computer Review*, 37(1), 38–54. https://doi.org/10.1177/0894439317734157

Bertolin, G. (2017) Digital Hydra: Security Implications of False Information Online. *NATO StratCom COE*. https://www.stratcomcoe.org/digital-hydra-security-implications-false-information-online

Bittman, L. y Godson, R. (1985). *The KGB and Soviet disinformation: an insider's view*. Pergamon-Brassey's.

Bittman, L. (1990). The use of disinformation by democracies. *International Journal of Intelligence and Counter Intelligence*, 4(2), 243-261. https://doi.org/10.1080/08850609008435142

Bontcheva, K., Posetti, J., Teyssou, D., Meyer, T., Gregory, S., Hanot, C., (2020) Balancing Act: Countering Digital Disinformation While Respecting

Freedom of Expression. *United Nations Educational, Scientific and Cultural Organization.* https://www.broadbandcommission.org/Documents/working-groups/FoE_Disinfo_Report.pdf

COGSEC-Collaborative. (2022). *Amitt (adversarial misinformation and influence tactics and techniques) framework for describing disinformation incidents. includes TTPS and countermeasures.* GitHub, https://github.com/cogsec-collaborative/AMITT

Colom-Piella, G. (2020). Anatomía de la desinformación rusa. *Historia y Comunicación Social*, 25(2), 473-480. https://doi.org/10.5209/hics.63373

Comisión Europea. (2018). *Final report of the High-Level Expert Group on Fake News and Online Disinformation*. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-andonline-disinformation

Comisión Europea. (2018). *Flash Eurobarometer 464: Fake News and Disinformation Online*. https://data.europa.eu/data/datasets/s2183_464_eng?locale=en

Comisión Europea. (2019). *Tackling online disinformation*. https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

Comisión Europea. (2020). *Plan de Acción para la Democracia Europea (EDAP).* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0790&from=ES

Edelman. (2021). *Trust Barometer* https://www.edelman.com/trust/2021-trust-barometer

Facebook. (2021). *Threat Report: The State of Influence Operations 2017-2020* https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday*, 22(8). https://doi.org/10.5210/fm.v22i8.8005

Galdón, G. (1994). *Desinformación: método, aspectos y soluciones*. Eunsa

Gelfert, A. (2018). Fake News: A Definition. *Informal Logic,* 38 (2), 84-117. https://doi.org/10.22329/il.v38i1.5068

Germani, F. y Biller-Andorno, N. (2021). The anti-vaccination infodemic on social media: A behavioral analysis. *PLOS ONE*, 16(3). https://doi.org/10.1371/journal.pone.0247642

House of Commons Digital, Culture, Media and Sport Committee. (2019). *Disinformation and 'fake news': Final Report* https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

Ingram, H.J. (2020). The Strategic Logic of State and Non-State Malign 'Influence Activities'. *The RUSI Journal*, 165, 12-24. https://doi.org/10.1080/03071847.2020.1727156

Jordán, J. (2018). El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo. *Revista Española De Ciencia Política*, 48, 129-151. https://doi.org/10.21308/recp.48.05

Jowett, G. y O'Donnell, V. (2011). *Propaganda and Persuasion*. SAGE Publications.

Kahn, I. (2021). *Disinformation and freedom of opinion and expression.* (A/HRC/47/25). United Nations. https://undocs.org/A/HRC/47/25

Kessler, G., Rizzo, S. y Kelly, M. (24 enero, 2021). Trump's false or misleading claims total 30,573 over 4 years. *Washington Post*. https://www.washingtonpost.com/politics/2021/01/24/trumps-false-or-misleading-claims-total-30573-over-four-years/

Khaldarova, I., y Pantti, M. (2016). Fake news: The narrative battle over the Ukrainian conflict. *Journalism Practice*, 10(7), 891-901. https://doi.org/10.1080/17512786.2016.1163237

Klein, D. O., Wueller, J. R. (2018). Fake News: A legal perspective. *Australasian Policing*, 10(2), 11-15, 17. https://search.informit.org/doi/10.3316/informit.807638896756480

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Zittrain, J. L. (2018). The science of fake news. *Science*, 359, 1094–1096. https://doi.org/10.1126/science.aao2998

Lewandowsky, S., Stritzke, W. G. K., Freund, A. M., Oberauer, K., y Krueger, J. I. (2013). Misinformation, disinformation, and violent conflict: From Iraq and the "War on Terror" to future threats to peace. *American Psychologist*, 68(7), 487–501. https://doi.org/10.1037/a0034515

Loomba, S., de Figueiredo, A., Piatek, S. J., de Graaf, K., y Larson, H. J. (2021). Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA. *Nature Human Behaviour*, 5, 337-348. https://doi.org/10.1038/s41562-021-01056-1

Magallón, R. (2019). *UnfakingNews: Cómo combatir la desinformación*. Ediciones Pirámide.

Manjoo, F. (5 de junio, 2017). La falsa realidad creada por los bots en Twitter. *The New York Times*. https://www.nytimes.com/es/2017/06/05/la-falsa-realidad-creada-por-los-bots-en-twitter/

Mayoral, J., Parratt, S. y Morata, M. (2019). Desinformación, manipulación y credibilidad periodísticas: una perspectiva histórica. *Historia y Comunicación Social*, *24*(2), 395-409 https://doi.org/10.5209/hics.66267

Merriam-Webster Dictionary. (2018). The real story of fake news. https://www.merriam-webster.com/words-at-play/the-real-story-of-fake-news

Molina, MD., Sundar, SS., Le, T., y Lee, D. (2021) "Fake News" Is Not Simply False Information: A Concept Explication and Taxonomy of Online Content. *American Behavioral Scientist,* 65(2),180-212. https://doi.org/10.1177/0002764219878224

Newman, N., Fletcher, R., Kalogeropoulos, A., Levy, D., Nielsen, R.K. (2017). Reuters Institute Digital News Report 2017. *Reuters Institute for the Study of Journalism*. https://reutersinstitute.politics.ox.ac.uk/our-research/digital-news-report-2017

Nielsen, R. K. y Graves, L. (2017). *News you don't believe: Audience perspectives on fake news*. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-10/Nielsen%26Graves_factsheet_1710v3_FINAL_download.pdf

Olmo y Romero, J.A. (2019). *Desinformación: concepto y perspectivas.* (ARI 41/2019) Real Instituto Elcano. https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari41-2019-olmoromero-desinformacion-concepto-y-perspectivas.pdf

OpenCTI-Platform, (2022). *OpenCTI-platform/opencti: Open cyber threat intelligence platform*. GitHub. https://github.com/OpenCTI-Platform/opencti

Oasis-Open, (2022). *Oasis-open/CTI-python-STIX2: Oasis TC open repository: Python apis for stix 2*. GitHub. https://github.com/oasis-open/cti-python-stix2

Quandt, T., Frischlich, L., Boberg, S., Schatto-Eckrodt, T. (2019). Fake News. *The international encyclopedia of journalism studies*, 1-6. https://doi.org/10.1002/9781118841570.iejs0128

Recuero, R., Soares, F., y Vinhas, O. (2020). Discursive strategies for disinformation on WhatsApp and Twitter during the 2018 Brazilian presidential election. *First Monday*, 26(1). https://doi.org/10.5210/fm.v26i1.10551

Repucci, S., y Slipowitz, A., (2021). *Democracy under Siege*. Freedom House. https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege

Ricard, J., y Medeiros, J. (2020). Using misinformation as a political weapon: COVID-19 and Bolsonaro in Brazil. *Harvard Kennedy School (HKS) Misinformation Review, 1(2)*. http://nrs.harvard.edu/urn-3:HUL.InstRepos:42661741

Rid, T. (2020). *Active Measures. The Secret History of Disinformation and Political Warfare*. Farrar, Straus & Giroux.

Rietjens, S. (2019). Unraveling disinformation: the case of Malaysia Airlines flight MH17. *The International Journal of Intelligence, Security, and Public Affairs*, 21(3), 195-218. https://doi.org/10.1080/23800992.2019.1695666

Rini, R. (2017). Fake News and Partisan Epistemology. *Kennedy Institute of Ethics Journal,* 27(2), E-43-E-64. https://muse.jhu.edu/article/670860

Robinson, L., Helmus, T., Cohen, R., Nader, A., Radin, A., Magnuson, M., y Migacheva, K. (2018). *Modern Political Warfare. Current Practices and Possible Responses*. Rand Corporation. https://doi.org/10.7249/RR1772

Rodríguez Pérez, C. (2019). No diga fake news, di desinformación: una revisión sobre el fenómeno de las noticias falsas y sus implicaciones. *Comunicación*, (40), 65-74. https://doi.org/10.18566/comunica.n40.a05

Rogers, Z., Bienvenue, E., y Kelton, M. (1 de mayo, 2019) The New Age of Propaganda: Understanding Influence Operations in the Digital Age. *War on the Rocks*. https://warontherocks.com/2019/05/the-new-age-of-propaganda-understanding-influence-operations-in-the-digital-age/

Salaverría, R., Buslón, N., López-Pan, F., León, B., López-Goñi, I., y Erviti, M. C. (2020). Desinformación en tiempos de pandemia: tipología de los bulos sobre la Covid-19. *Profesional de la información*, 29(3). https://doi.org/10.3145/epi.2020.may.15

Salaverría-Aliaga, R. (2021). Entender y combatir la desinformación sobre ciencia y salud. *Ministerio de Ciencia e Innovación*. https://hdl.handle.net/10171/60223

Schwirtz, M. y Bautista, J. (3 septiembre, 2021). Married Kremlin Spies, a shadowy mission to Moscow and unrest in Catalonia. *The New York Times*. from https://www.nytimes.com/2021/09/03/world/europe/spain-catalonia-russia.html

Singer, P. W. y Brooking, E. T. (2018) LikeWar: The Weaponization of Social Media, Eamon Dolan/Houghton Mifflin Harcourt, New York.

Sipher, J. (13 de Agosto, 2018). Convergence Is Worse Than Collusion. *The Atlantic*. https://www.theatlantic.com/ideas/archive/2018/08/convergence-is-worse-than-collusion/567368/

Snyder, A. (1997). *Warriors of disinformation: American propaganda, Soviet lies, and the winning of the Cold War: an insider's account*. Arcade Publishing.

Swire, B., Berinsky, A. J., Lewandowsky, S., y Ecker, U. K. (2017). Processing political misinformation: comprehending the Trump phenomenon. *Royal Society Open Science*, 4(3), 160802. https://doi.org/10.1098/rsos.160802

Tandoc Jr. E.C., Lim, Z. W. y Ling, R. (2018). Defining "fake news" A typology of scholarly definitions. *Digital Journalism*, 6(2), 137-153. https://doi.org/10.1080/21670811.2017.1360143

Tandoc Jr. E.C., Thomas, R. y Bishop, L. (2021). What is (fake) news? Analyzing news values (and more) in fake stories. *Media and Communication*, 9(1), 110-119. https://doi.org/10.17645/mac.v9i1.3331

Torreblanca, J.I. (2020). Democracia y redes sociales. En V. Lapuente y E. Costas (Coords.), *Cómo salvar las democracias liberales* (131-166). Círculo de Empresarios

Wardle, C. y Derakhshan, H. (2017). *Information disorder toward an interdisciplinary framework for research and policymaking* (DGI(2017)09),

Consejo de Europa. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Weedon, J., Nuland, W., y Stamos, A. (2017). *Information Operations and Facebook*. Facebook. https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf

Wu, T. (2016). *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*. Random House, New York.

CAPÍTULO 2

PROPUESTAS DE REGULACIÓN ANTE LA DESINFORMACIÓN

Coordinador sociedad civil:

Lorenzo Cotino Hueso (Plataforma en Defensa de la Libertad de Información)

Coordinador institucional:

Ministerio del Interior – Secretaria de Estado de Seguridad

Autores y colaboradores:

Ofelia Tejerina Rodríguez (Asociación de Internautas)

José Domingo Gómez Castallo (Asociación para la Autorregulación de la Comunicación Comercial)

Hilda Garrido Suárez (Consejo General de la Abogacía Española)

Guillermo Serrano Peña (Facebook)

Aurelio Martín González (Federación de Asociaciones de Periodistas de España)

Javier Castro-Villacañas (Federación de Asociaciones de Radio y Televisión de España)

Ana Abade Gil (Google)

Santiago Menéndez-Abascal Cabiedes (Google)

Carlos Hernández-Echevarría Monge (Maldita.es)

Gabriel López Serrano (Microsoft)

Marta López López (Reporteros Sin Fronteras)

Ángel Vallejo Chamorro (Thiber)

Camino Rojo Torres (Twitter)

EL CONTEXTO DE LA REGULACIÓN DE LA DESINFORMACIÓN Y POSICIÓN GENERAL REGULATORIA

Los conceptos de desinformación manejados normativamente en otros países

El capítulo uno se centra en el fenómeno y concepto de los desórdenes informativos y la desinformación, y en su caso, delimitando las influencias indebidas extranjeras, las operaciones de influencia estructuradas y elementos como el comportamiento de los sujetos que las producen más allá de los contenidos que se difunden. A los resultados del referido capítulo cabe remitirse. En cualquier caso, desde la perspectiva jurídico normativa la delimitación del concepto de la desinformación y los desórdenes informativos es esencial por cuanto a las implicaciones concretas que pueden derivar. Es más, si se trata de una respuesta penal o sancionadora al fenómeno desinformativo, los conceptos deben ser más concretos y restrictivos si cabe por su mayor impacto en libertades, derechos y principios democráticos.

Si se trata de una respuesta penal o sancionadora al fenómeno desinformativo, los conceptos deben ser más concretos y restrictivos si cabe por su mayor impacto en libertades, derechos y principios democráticos.

Resulta útil recordar algunas delimitaciones legislativas del concepto en países democráticos. Previamente al fenómeno digital, cabe destacar dos normas francesas. Así, el artículo 27 de la Ley del 29 de julio de 1881 de Francia sobre la libertad de prensa, castiga "la publicación, distribución o reproducción, por cualquier medio, de noticias falsas, de partes fabricadas, falsificadas o engañosamente atribuidas a

terceros cuando, hecha de mala fe, haya perturbado la paz pública, o haya sido susceptible de perturbarlo, será castigado con una multa de 45,000 euros".

El artículo L97 del Código Electoral francés también permite procesar a alguien por difundir noticias falsas: "Quienes, con ayuda de noticias falsas, rumores difamatorios u otras maniobras fraudulentas, hayan sorprendido o desviado votos, determinaron que uno o más votantes se abstuvieran votantes, será sancionado con un año de prisión y multa de 15.000 euros".

Es preciso señalar que respecto de esta legislación francesa la jurisprudencia ha sido muy restrictiva y son muy extrañas las condenas por aplicación de estos preceptos.

Para el fenómeno de la desinformación en el mundo digital, hay que destacar la Loi n° 2018-1202 de 22 de diciembre de 2018 de lucha contra la manipulación de información. La misma permite que un juez en 48 horas pueda determinar la retirada o bloqueo de contenidos tres meses antes de las elecciones, en concreto "acusaciones o imputaciones que sean inexactas o engañosas (*allégations ou imputations inexactes ou trompeuses*) en cuanto a un hecho que pueda alterar la transparencia de la próxima votación y que se difunden de forma deliberada, artificial o automatizada y masiva a través de un servicio de comunicación pública en línea".

El Consejo Constitucional en su decisión de 20 de diciembre de 2018 al interpretar esta ley exige garantías, como que sea "posible demostrar la falsedad de forma objetiva" se justifique su carácter "manifiesto" y que no se trate de "opiniones, parodias, inexactitudes parciales o simples exageraciones". Asimismo, el Consejo Constitucional ha exigido que se justifique que la inexactitud o confusión "es obvia" y que sea "manifiesto" el "riesgo de alterar la transparencia de la votación". Estos elementos conceptuales de esta norma interpretada según el Consejo Constitucional pueden ser un buen punto de partida desde el punto de vista jurídico para determinar sobre qué tipo de alteración de la información puede actuarse. Y debe recordarse que este ejemplo legislativo no es para permitir una persecución sancionador o penal. En estos casos, si cabe, el fenómeno de desinformación aún debe interpretarse de modo más restrictivo.

En Canadá, la Elections Modernization Act, dec. 13, 2018 (BILL C-76) regula la «undue influence by foreigners» (282. 4 (1). Ahí se prohíbe en general la «influencia indebida por parte de extranjeros» para las votaciones y gastos. No obstante, debe señalarse que las excepciones son muy amplias y permiten

a extranjeros opinar o hacer reportajes a favor de unos resultados o a favor de candidatos.

La reciente propuesta legislativa de Reino Unido de 12 de mayo de 2021 (*Online Safety Bill*) incluye la desinformación entre los posibles "daños" frente a los que las grandes plataformas obligatoriamente deben tomar medidas. La delimitación misma del daño ya supone una cuestión muy controvertida y criticada por ser contraria a la libertad de expresión. En cualquier caso y para restringir el concepto, el Comité de la Cámara de los Lores ya ha insistido en que los daños "tienen que resultar en un daño a la persona: esto lleva a la exención de amplias franjas de daños a la sociedad que son el resultado de campañas coordinadas o cuando la agregación de daños individuales es tal que se produce un daño social distinto".

Así pues, como puede apreciarse, los conceptos recogidos en los países democráticos en normas para dar respuesta a la desinformación han de ser muy concretos y restrictivos. Estos conceptos necesariamente dejan fuera muchas realidades que comúnmente se identifican como desinformación frente a las cuales, como punto de partida, no cabe reacción legal alguna en los países democráticos.

La concrección y restricción de los conceptos necesariamente dejan fuera muchas realidades que comúnmente se identifican como desinformación frente a las cuales, como punto de partida, no cabe reacción legal alguna en los países democráticos.

Por el contrario, los países que no cumplen o sólo relativamente los mínimos estándares democráticos, regulan el fenómeno de la desinformación con conceptos pretendidamente amplios que en modo alguno son admisibles. Así, son claros ejemplos a no seguir en ningún caso, los ejemplos regulatorios de países no democráticos en leyes o proyectos de ley que criminalizan difundir "propaganda" o el contenido "agresivo y aterrador" (Bangladesh); difundir información falsa en línea (Bielorrusia), o éstos se considera que "amenazan la seguridad nacional" (Camboya). También se criminaliza reportar "cualquier noticia sin poder demostrar su verdad o que tiene una buena razón para creer que es verdad" (Camerún); "difundir información falsa a sabiendas" (Kazajstán o Kenia); "fake news" (Egipto); la publicación de "información incorrecta" que cause "temor o alarma al público" (Myanmar).

Otro ejemplo destacable a no seguir es el de Rusia. La Ley Federal del 18 de marzo de 2019 N 30-ФЗ "protección de la información" regula "el procedimiento para restringir el acceso a información indecente que atenta contra la dignidad

humana y la moral pública, evidente falta de respeto a la sociedad". En varios casos, se sanciona "la difusión en los medios de comunicación, así como en las redes de información y telecomunicaciones de información inexacta de importancia social a sabiendas bajo la apariencia de mensajes confiables". Y ello se acompaña con la Ley Federal del 1 de mayo de 2019 N 90-ФЗ, conocida como "ley de RuNet soberana" o la "ley sobre la internet segura". Por lo que interesa, un órgano administrativo puede tomar el control de todo internet en Rusia si declara que hay una situación de emergencia en razón de una campaña de desinformación.

Posición general regulatoria a partir de los presupuestos internacionales y de la Unión Europea

El Grupo desde su inicio ha partido de una posición general regulatoria muy cautelosa. Se considera que son un ejemplo a no seguir las experiencias de muchos países que dudosamente cumplen los estándares mínimos de democracia y libertades públicas. En esencia, se debe huir de una criminalización general del fenómeno por la grave dificultad de definir el mismo con la precisión necesaria para que la regulación sea efectiva. Cuestión diferente es que algunas de las manifestaciones más concretas de la desinformación sí puedan ser objeto de regulación o ya estén criminalizadas en la legislación vigente (delitos de odio, revelación de secretos, contra la integridad moral, desórdenes públicos, injurias y calumnias, contra la salud pública, estafas, intrusismo, contra el mercado y los consumidores, ver Fiscalía General del Estado, Tratamiento penal de las "Fake news" 2020).

Se debe huir de una criminalización general del fenómeno por la grave dificultad de definir el mismo con la precisión necesaria para que la regulación sea efectiva.

El abordaje de la desinformación desde un punto de vista normativo puede hacerse desde diversas perspectivas.

El uso de normas jurídicas es limitado. Los estándares internacionales en materia de libertad de expresión[1], establecen que una criminalización o simple ilegalización de información simplemente etiquetada como "falsa" es incompatible con el Derecho internacional de los derechos humanos por otorgar a los Estados y a sus autoridades la potestad discrecional de determinar la verdad o la falsedad acerca de temas sociales relevantes. Dicho informe señala:

> «83. […] Por ello, los intentos de combatir la desinformación socavando los derechos humanos son cortos de miras y contraproducentes. El derecho a la libertad de opinión y de expresión no es parte del problema, sino el objetivo y el medio para combatir la desinformación. La pandemia de COVID-19 ha puesto de manifiesto tanto la necesidad esencial de defender el derecho como las complicaciones que supone hacer frente a la desinformación y la información errónea. […]

[1] Ver particularmente el Informe A/HRC/47/25 de abril 2021 (Naciones Unidas [NN. UU.], 2021) presentado por la relatora especial de libertad de expresión Irene Khan ante el Consejo de Derechos Humanos de Naciones Unidas.

> 85. La desinformación es problemática, pero también lo son las respuestas de los Estados y las empresas. Muchas leyes y políticas se están elaborando con un conocimiento insuficiente de los perjuicios que se causan en Internet, sin datos, investigaciones o consultas públicas adecuadas. Distintos Estados han recurrido a medidas desproporcionadas como cierres de Internet y leyes vagas y demasiado poco específicas. Estas medidas no solo son incompatibles con el derecho internacional de los derechos humanos, sino que también contribuyen a amplificar las percepciones erróneas, fomentando el miedo e incrementando la desconfianza de la ciudadanía en las instituciones.»

Que una eventual regulación de la desinformación resultaría una tarea compleja por su injerencia en otros derechos y libertades lo acredita la Sentencia de 25 de julio de 2019 (Asunto Brzezinski contra Polonia)[2] del Tribunal Europeo de Derechos Humanos (TEDH). En esta sentencia, el tribunal apreció por unanimidad una infracción de la libertad de expresión reconocida en el Convenio como consecuencia de la aplicación de una previsión de la ley electoral polaca en virtud de la cual un tribunal había prohibido la distribución de un folleto electoral que incluía información falsa.

Con todo, y con el fin de evitar fragmentación y desarmonización, tampoco nos parece prudente abordar el fenómeno de la desinformación de espaldas a las siguientes iniciativas en curso en el marco de la Unión Europea:

- El Plan de Acción para la Democracia Europea (Comisión Europea, 2020), publicado el 3 de diciembre de 2020.
- El Código de buenas prácticas de la Unión en materia de desinformación (Comisión Europea, 2018) que, en el momento de escribir estas líneas, se encuentra en proceso de revisión (Comisión Europea, 2021) y abierto a nuevos participantes.
- La propuesta de reglamento conocida como Ley de Servicios Digitales (Comisión Europea, 2020b).
- La propuesta de legislación para garantizar una mayor transparencia en el ámbito del contenido patrocinado en un contexto político (Comisión Europea, 2021d, 2021e).

---

[2] Ver en http://hudoc.echr.coe.int/eng?i=001-194958

Asimismo, hay que ser especialmente cautelosos con las regulaciones ya sean penales o sancionadoras del ámbito de las comunicaciones o similares en las que una autoridad gubernativa define esencialmente las actividades a prohibir, sancionar, bloquear, etc. Pese a las apariencias de regulaciones garantistas, es de gran riesgo que una autoridad de naturaleza gubernativa o administrativa defina las acciones, prácticas o contenidos a restringir por ser "desinformación". Si alguna autoridad ha de llevar a cabo estas evaluaciones con posibles consecuencias restrictivas debe ser de naturaleza judicial. Asimismo, la Junta Electoral es un órgano que ya cuenta con competencias específicas que, como más adelante se apunta, deben ser aclaradas y reforzadas. Sin embargo, pese a la jurisprudencia del TC, se consideraría inadecuado reconocer estas facultades a órganos reguladores del ámbito audiovisual. Para el caso de que se decidiera reconocer facultades a autoridades, debería en todo caso garantizarse que sean auténticamente independientes y en su caso que en su composición se garantice un peso de integrantes de naturaleza judicial, así como de procedencia de la sociedad civil y sin participación decisoria de miembros de procedencia gubernamental o administrativa.

Es de gran riesgo que una autoridad de naturaleza gubernativa o administrativa defina las acciones, prácticas o contenidos a restringir por ser "desinformación".

En la lucha contra la desinformación desde hace años están siendo esenciales los esfuerzos y el papel de las plataformas e intermediarios (ver Anexo). Obviamente, cada una de ellas con sus propias políticas, prácticas y procedimientos para atajar y contrarrestar la desinformación. Frente a regulaciones *fuertes* que establezcan obligaciones y restricciones de contenidos o impongan concretas obligaciones de actuación de los intermediarios, se considera que diversos modos de autorregulación o corregulación pueden encauzar efectivamente el fenómeno, asimismo estos modelos permiten complementar las regulaciones existentes y hacerlas más efectivas. Con el fin de garantizar la armonización y unidad de acción y criterios es imprescindible que toda propuesta regulatoria parta del marco de la UE y especialmente hay que tener en cuenta el ya mencionado Código de Buenas Prácticas contra la desinformación de la UE. Los fenómenos de autorregulación de las plataformas, intermediarios u otros actores implicados, obviamente deben tener en cuenta y en su caso complementar la regulación existente. En este punto, en la medida en la que fuera aplicable, el Grupo de Trabajo ha tenido en cuenta la propuesta de Digital Services Act (DSA).

El Grupo también es favorable a que existan instituciones, órganos y funciones definidas normativamente en el ámbito gubernamental para identificar, detectar y monitorear el fenómeno de la desinformación. De igual modo, resulta procedente determinar algunos mecanismos de protección frente al mismo bajo el enfoque de la ciberseguridad y la ciberdefensa. En esta misma línea, también debe existir una mayor coordinación de acciones de respuesta entre las entidades competentes. Deben asimismo reforzarse los marcos de cooperación interna tanto con el sector público, como con la sociedad civil, la academia, las entidades de verificación de datos y el sector privado.

El Grupo también es favorable a que existan instituciones, órganos y funciones definidas normativamente en el ámbito gubernamental para identificar, detectar y monitorear el fenómeno de la desinformación.

En este sentido, el Grupo se congratula del establecimiento de mecanismos de colaboración entre el Gobierno y la sociedad civil contemplados en la Orden PCM/1030/2020, de 30 de octubre, sobre el Procedimiento de actuación contra la desinformación (Boletín Oficial del Estado [BOE], 2020) aprobado por el Consejo de Seguridad Nacional (CSN) y anima a su desarrollo y consolidación para una mayor colaboración y eficacia en la lucha contra las campañas de desinformación. Esta regulación orgánica, competencial y funcional de las instituciones internas españolas también es necesaria para articular la acción concertada con la UE y en otros marcos internacionales.

También se considera que hay terrenos acotados en los que el Derecho puede intervenir con mayor precisión y quizá menores riesgos frente a la difusión de desinformación. No hay que excluir las regulaciones especiales para hacer frente al fenómeno de la desinformación en determinados ámbitos, como la legislación sanitaria y de consumo con relación a determinados productos y tratamientos, así como en el ámbito de la protección de menores o colectivos con habilidades especiales.

Presupuestos regulatorios desde las libertades informativas

Este grupo ha tenido especialmente en cuenta la visión general del fenómeno en el marco de Naciones Unidas y en especial por los relatores de libertad de expresión. Se considera un acertado punto de partida el general de Estados Unidos que huye de cualquier valoración de contenidos por las autoridades que pueda suponer orquestar el debate político. Allí, desde 1927 la "Counterspeech Doctrine" establecida por Brandeis viene a suponer que frente a la mentira lo que procede es la deliberación y más libertad de expresión, pero en modo alguno orquestar el debate por los poderes públicos. Así lo expresa en 2012 el juez Kennedy en Estados Unidos. v. Alvarez:

> "El remedio para el discurso que es falso es el discurso que es verdadero. Este es el curso ordinario en una sociedad libre. La respuesta a lo irracional es lo racional; a los desinformados, a los iluminados; a la mentira directa, la simple verdad… La sociedad tiene el derecho y el deber cívico de participar en un discurso abierto, dinámico y racional. Estos fines no están bien atendidos cuando el gobierno busca orquestar la discusión pública a través de mandatos basados en contenido".

En esta dirección[3], cabe señalar como ya advirtieron los relatores internacionales para la libertad de expresión en su Declaración conjunta de marzo de 2017, buena parte de las medidas legales que se han dado en el mundo frente a la desinformación (entre otros, estudios Congreso EE. UU.), no son otra cosa que la criminalización del rival u opositor político y no superan los mínimos estándares jurídicos democráticos.

La muy amplia e intensa protección de la libertad de expresión por la jurisprudencia europea y española no alcanza a proteger un derecho a mentir, pero sí que teóricamente imposibilita el control de la verdad o mentira de las opiniones y dificulta mucho el control de la veracidad de informaciones impregnadas de la libertad de expresión. Así, el Tribunal Constitucional español ha señalado que afirmaciones como que las cámaras de gas no existen no quedan bajo el análisis de la libertad de información, esto es, que no están sometidas al criterio de la veracidad, sino que son una manifestación de la libertad de expresión (ello sin perjuicio de que finalmente considerara que eran afirmaciones

[3] (Library Of Congress [LOC], 2019, 2019b)

contrarias a la dignidad humana). Asimismo, la libertad de expresión sí que protege muchas formas de interpretar los hechos en una sociedad democrática (TEDH, Handyside v. Reino Unido 1976). Especialmente en el ámbito político se protegen las exageraciones (TEDH, Renaud v. France, 2010) y no hay que probar la verdad de los juicios críticos (Dalban v. Romania, 1999). El Grupo considera que la variada jurisprudencia del TEDH no facilita en general aplicar el artículo 17 del Convenio Europeo de Derechos Humanos (CEDH) para tomar medidas frente a la desinformación. Y es que se podría argumentar que algunos fenómenos de desinformación suponen el abuso del derecho a informar. Ello permitiría legitimar medidas restrictivas en la prohibición de abuso de derecho contra el sistema democrático de los artículos 17 CEDH y 54 de la Carta de Derechos fundamentales de la UE. Frente a esta argumentación, se considera que sólo cabría seguir esta vía en casos muy evidentes y claramente vinculados a delitos de odio y siempre con la interpretación restrictiva que el TEDH exige respecto de estos delitos.

Debido al difícil equilibrio entre regular la desinformación y respetar la libertad de expresión, son opciones muy importantes: impulsar la visibilidad y alcance de fuentes de información legítimas, una mayor colaboración entre las plataformas digitales, los *fact-checkers,* sociedad civil e instituciones, así como una adecuada formación en alfabetización mediática que otorgue a la ciudadanía las herramientas y conocimientos adecuados para pensar de manera crítica.

Foto 3: Sede del Tribunal Constitucional, en Madrid. EFE/Zipi

Algunas inercias regulatorias en España

Acertadamente, desde la Estrategia de Seguridad Nacional 2017 se incluyen los ciberataques y las campañas de desinformación. También desde la Proposición no de ley de derechos digitales y veracidad de las informaciones de 27 de marzo de 2017 se han dado algunos intentos en la regulación del fenómeno de la desinformación en España. Esta proposición fue retomada en la Ley Orgánica 3/2018 a través de una enmienda. Se pretendió que "los responsables de redes sociales, plataformas digitales y servicios equivalentes de la sociedad de la información garantizarán la veracidad informativa" y para ello habían de adoptar medidas para protocolos efectivos para "previa queja o aviso, eliminar contenidos". Dicha propuesta fue contestada desde la sociedad civil y el precepto finalmente adoptado limitó mucho su campo de acción al ser sólo relativo al derecho de rectificación en internet (artículo 85). De hecho, en más de tres años no parece que se hayan adoptado o hayan sido necesarios "protocolos adecuados para posibilitar" este derecho como ahí se prescribe.

La ya aludida Orden PCM/1030/2020, de 30 de octubre, publica el Procedimiento de actuación contra la desinformación aprobado por el CSN. Esta orden generó una importante controversia política pese a que la misma no establece medidas concretas sobre la moderación de contenidos. Establece una estructura gubernamental para coordinar acciones de monitorización, detección y reacción temprana ante campañas de desinformación. Asimismo, introduce mecanismos para una mayor cooperación con expertos, sociedad civil, la comunidad de verificadores de datos y plataformas digitales para reaccionar ante dichas campañas organizadas, lo cual, como se menciona anteriormente, este grupo saluda y anima a su desarrollo y consolidación. La sentencia del Tribunal Supremo (TS) de 18 de octubre de 2021 ha inadmitido el recurso presentado frente a la Orden[4]. Frente a los recursos presentados a la Orden, el TS aprecia positivamente los objetivos de la orden y se sostiene que el CSN está normativamente apoderado para elaborar y aprobar un instrumento de actuación con facultades de coordinación. Asimismo, se indica que la orden "no es una norma sustantiva o de conducta, sino de estructura o competencia" y que "el procedimiento impugnado no incurre en ninguna restricción ni vulneración de los derechos fundamentales del artículo 20 de la CE".

[4] Tribunal Supremo (2021). Sentencia nº 1240/2021, de 18 de octubre de 2021 Sala de lo Contencioso, Sección 4, Rec 361/2020 y Tribunal Supremo (2021). Sentencia nº 1238/2021, de 18 de octubre de 2021 Sala de lo Contencioso, Sección 4, Rec 384/2020

Sin tratarse de un texto de carácter normativo, cabe mencionar la Carta de Derechos digitales adoptada en julio de 2021, la cual contiene algunos elementos de interés para el ámbito de la desinformación.

Foto 4: Sede del Tribunal Supremo, en Madrid. EFE/Emilio Naranjo

PROPUESTAS REGULATORIAS

Regulación institucional y orgánica de la desinformación

El Grupo ha subrayado que es esencial que existan mecanismos de transparencia y control. En el ámbito de las instituciones del Estado respecto del fenómeno de las campañas de desinformación se considera importante dotar al sistema de una gobernanza adecuada con participación y transparencia. La Orden de 2020 es un primer paso que debe fortalecerse. En esta dirección, y dada además la especial sensibilidad social en la materia, la transparencia es muy importante. La futura institucionalización y ordenación debería concretar la necesidad de elaborar informes de las acciones realizadas por los órganos públicos con responsabilidades en la materia y periodicidad y la publicidad activa de los mismos. También debería aclararse si la información o documentación generada tiene en su caso una particular reserva y confidencialidad, que sólo debe darse en lo que sea

Es esencial que existan mecanismos de transparencia y control.

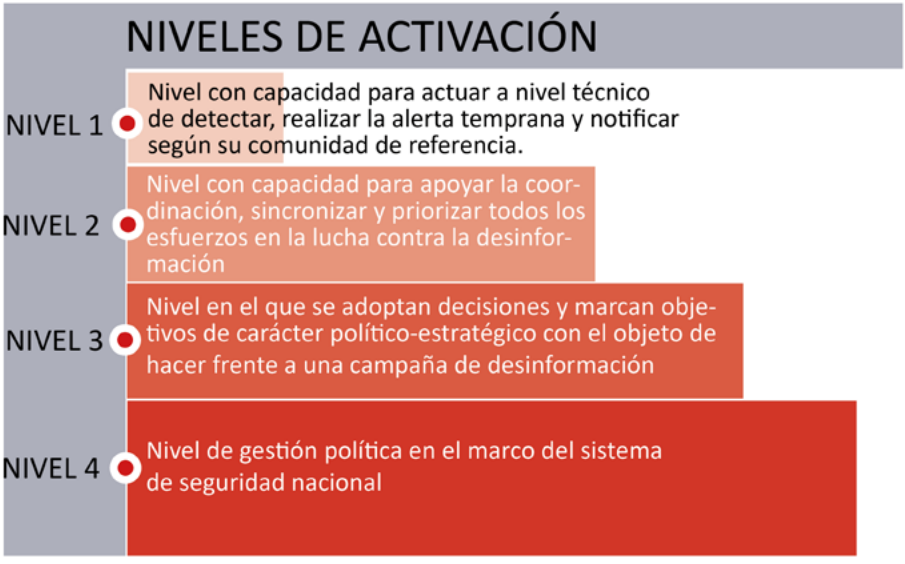


Gráfico 3: Procedimiento de lucha contra la desinformación: niveles de activación
Elaborado por el DSN

necesario por razones de eficacia y seguridad y en el marco de la legislación aplicable.

Asimismo, se considera muy positivamente la creación, existencia y participación de comités de expertos independientes que integren a la sociedad civil, a los sectores especialmente involucrados, así como a personas expertas y del ámbito académico. En razón del tipo de ente u órgano puede ser especialmente positiva su integración por miembros del poder judicial o de autoridades independientes afines a la materia.

La participación de agentes externos a la acción gubernamental es una garantía y mecanismo de control que debe ser estimulado. El deber de secreto y confidencialidad que pueden requerir ciertas materias puede ser jurídicamente asegurado y no debe ser excusa.

En la línea de lo ya afirmado, se considera oportuno el desarrollo de los instrumentos de cooperación y colaboración entre el gobierno y la academia, la comunidad de verificadores de datos, las plataformas digitales y otros expertos de la sociedad civil que introduce la Orden de 2020. Ello debe generar positivas dinámicas de interlocución y compartición de información.

Este grupo de trabajo reconoce los amplios esfuerzos que se están realizando desde algunas de las principales plataformas, no sólo por su participación en mecanismos de compartición, también por el establecimiento de sistemas voluntarios de transparencia. En todo caso, en el contexto de la actualización del Código europeo de Buenas Prácticas contra la desinformación de la UE damos la bienvenida al actual proceso de análisis y revisión de tales mecanismos de transparencia y la mucha información que se pone a disposición que se está llevando a cabo. Esta revisión del Código europeo puede establecer unos elementos básicos y mínimos para lograr que la información que se facilita llegue efectivamente a los actores principales y que incluya la información usable y de utilidad sobre el fenómeno. Como es obvio, la regulación que delimite los instrumentos y contenidos de transparencia habrá de tener en cuenta las exigencias de protección de datos y las suficientes salvaguardas para evitar que agentes maliciosos puedan eludir o burlar los protocolos, tácticas o mecanismos de detección y respuesta adoptados por las plataformas para combatir la desinformación.

Propuestas regulatorias vinculadas a amenazas internacionales, a la ciberdefensa y a la cooperación con la UE

Las campañas de desinformación pueden constituir una amenaza a la seguridad tanto a nivel nacional como internacional. En perspectiva de Derecho internacional, este grupo de trabajo considera oportuno asentar algunas premisas. Así, España -como cualquier Estado soberano- tiene la facultad y el deber de combatir, en el marco de sus prerrogativas constitucionales, la difusión de noticias falsas o distorsionadas que puedan interpretarse como una injerencia en los asuntos internos de otros Estados o como perjudiciales para la promoción de la paz, la cooperación y las relaciones amistosas entre Estados. España reconoce el deber de abstenerse de toda campaña de difamación, vilipendio o propaganda hostil que tenga por fin intervenir o injerir en los asuntos internos de otros Estados.

España tiene la facultad y el deber de combatir, en el marco de sus prerrogativas constitucionales, la difusión de noticias falsas o distorsionadas que puedan interpretarse como una injerencia en los asuntos internos.

Una campaña organizada de desinformación puede constituir, dependiendo de su alcance, naturaleza y efectos, una violación de los principios de soberanía o de no intervención, o una amenaza, un uso de la fuerza, un ataque armado o una agresión contraria al Derecho Internacional. Conforme a la normativa en vigor, España puede adoptar las medidas necesarias para restaurar la legalidad y ejercer sus prerrogativas soberanas con relación a la atribución de las acciones y responsabilidades a un sujeto de Derecho Internacional o a cualquier agente a quien corresponda la autoría. A esos efectos, siguiendo los compromisos adoptados en el marco de Naciones Unidas, considerará toda la información pertinente, incluido el contexto más amplio del evento, los desafíos de atribución en el entorno de las TIC y la naturaleza y el alcance de las consecuencias.

Una campaña organizada de desinformación puede constituir, dependiendo de su alcance, naturaleza y efectos, una violación de los principios de soberanía o de no intervención, o una amenaza, un uso de la fuerza, un ataque armado o una agresión contraria al Derecho Internacional.

La acción contra las campañas de desinformación podrá implicar el ejercicio del derecho a la legítima defensa individual y colectiva en los términos y condiciones prescritos en el art. 51 de la Carta de Naciones Unidas y conforme a los acuerdos suscritos en materia de asistencia mutua en el Tratado de la Unión Europea y en el marco de la Organización del Tratado del Atlántico Norte.

La determinación de si una campaña organizada de desinformación constituye un problema de seguridad internacional se realizará en el marco de los órganos y conforme a los procedimientos establecidos en la Carta de Naciones Unidas y en cooperación y en cumplimiento de las obligaciones asumidas en el marco de las restantes organizaciones internacionales con competencias en la materia a las que pertenece España. Por su parte, la consideración de si constituye una amenaza a la seguridad nacional se realizará conforme a la normativa nacional.

La acción contra las campañas de desinformación se realizará conforme a los principios de la Carta de Naciones Unidas, en particular, los principios de igualdad soberana, arreglo pacífico de controversias, prohibición del uso o de la amenaza de la fuerza armada contra la integridad territorial o la independencia política de cualquier Estado y no intervención en los asuntos internos de otros Estados. La acción en materia de las campañas de desinformación se realizará individualmente o en cooperación con otros Estados y organizaciones internacionales competentes en la materia. A este respecto España trabaja y coopera especialmente con la Unión Europea y sus Estados miembros. En este contexto, la acción en materia de desinformación incluirá la promoción de medidas de transparencia, medidas de fomento de la confianza y medidas de creación de capacidades, así como el intercambio de información y buenas prácticas en el marco de las organizaciones y organismos competentes en la materia.

Hay que tener en cuenta el contexto normativo de la ciberseguridad y ciberdefensa que pueda estar vinculado o ser aplicable. Así, en especial cabe mencionar la Directiva 2016/1148, de 6 de julio, Directiva NIS (Security of Network and Information Systems) y su transposición en España (Real Decreto-ley 12/2018, de 7 de septiembre[5] y Real Decreto 43/2021, de 26 de enero[6]). Este conjunto puede especialmente afectar a operadores, intermediarios y plataformas españolas y en su caso puede estar relacionado con el fenómeno de las campañas de desinformación. El Real Decreto-Ley 14/2019[7], modificó el artículo 4. 6º de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones,

---

[5] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (BOE núm. 218, de 8 de septiembre de 2018, 87675-87696).

[6] Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de de septiembre, de seguridad de las redes y sistemas de información (BOE núm. 24, de 28 de enero de 2021, 8187-8214).

[7] Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones (BOE núm. 266, de 5 de noviembre de 2019).

Foto 5: Sesión plenaria del Parlamento Europeo en Estrasburgo (Francia). EFE/Thierry Suzan

en razón de la seguridad pública y nacional que permite la intervención y control gubernamental de los operadores de telecomunicaciones. El Tribunal Constitucional ha admitido un recurso de inconstitucionalidad del Gobierno Vasco frente al mismo.

El Grupo considera que la transparencia es el elemento esencial para generar confianza y que debe ser especialmente garantizada en periodo electoral respecto de los posibles ataques y operaciones de influencia masiva que puedan producirse si alcanzan un nivel muy relevante. En este sentido es un modelo positivo a tener en cuenta el "Protocolo público de incidentes electorales críticos" de marzo de 2019 en Canadá. Se trata de un proceso simple, claro e imparcial mediante el cual los canadienses deben ser notificados de una amenaza a la integridad de las elecciones. Cinco expertos del sector público, sólo en período

La transparencia es el elemento esencial para generar confianza y que debe ser especialmente garantizada en periodo electoral respecto de los posibles ataques y operaciones de influencia masiva.

electoral y bajo la especial neutralidad pública de este período (*Caretaker Convention*), tienen que determinar el origen y la importancia de incidentes. El protocolo incluye informar al Primer Ministro y otros líderes de partidos, candidatos, organizaciones o funcionarios electorales si han sido el objetivo conocido de un ataque. Los expertos pueden considerar que hay circunstancias excepcionales que pueden afectar a las elecciones y, si es así, deciden realizar una rueda de prensa para informar a toda la ciudadanía. El anuncio no aborda la fuente del ataque y no incluye información clasificada. Además, en su caso, se informa a los ciudadanos sobre los pasos para protegerse y las acciones adoptadas por el gobierno (no necesariamente con detalles). El Primer Ministro no puede vetar esta información.

Frente a influencias indebidas otros modelos regulatorios que conllevan la restricción de emisiones o bloqueo de contenidos son especialmente controvertidos. De un lado, pueden ser de dudosa utilidad. Así sucede en Canadá, donde la Elections Modernization Act, de 13 de diciembre de 2018 (BILL C-76), regula la «undue influence by foreigners» (282.4(1)) (Influencia indebida por parte de extranjeros). En principio, está prohibido que gobiernos, personas o empresas extranjeras influyan para que se vote o no se vote, en concreto se prohíbe hacer gastos a favor o en contra de un partido o líder. También si la influencia se da cometiendo algún delito regulado. Sin embargo, son muy grandes las excepciones al concepto de influencia indebida. Se permite como excepción expresar opiniones sobre el resultado, hacer declaraciones que animen a votar o no por candidatos. También se permiten informaciones, reportajes o editoriales sobre las elecciones de Canadá.

La regulación francesa de 2018 no es un modelo suficientemente probado ni trasladable a España y, cuanto menos, habría que analizar más detenidamente sus posibles efectos. Por lo que ahora interesa, esta ley introduce un artículo 33-1-1 en la Ley Nº 86-1067 del 30 de septiembre de 1986. El *Conseil supérieur de l'audiovisuel* en tres meses antes de elecciones tiene facultades para suspender emisiones de contenidos que son consecuencia de acuerdos con Estados extranjeros o están realizados "bajo su influencia". El *Conseil supérieur* también puede avisar y obligar a que medios dejen de emitir si consideran que están bajo órdenes o influencia de Estado extranjero contra "los intereses fundamentales de la Nación, incluido el funcionamiento regular de sus instituciones, en particular mediante la difusión de información falsa." ("*intérêts fondamentaux de la Nation, dont le fonctionnement régulier de ses institutions, notamment par la diffusion de fausses informations").* El Grupo considera que, si bien se podrían regular específicamente para periodo electoral atribuciones excepcionales, habrían de regularse con una ley que establezca claramente los presupuestos, las medidas concretas a adoptar y, especialmente, dejando en mano estas facultades a órganos de naturaleza judicial o a la junta electoral y siempre con suficientes cautelas y transparencia.

Propuestas regulatorias relativas al ámbito electoral

Este Grupo se remite al valioso trabajo específico del Capítulo 4, sin perjuicio de hacer las consideraciones del ámbito jurídico y de regulación que es propio a este grupo. En este sentido, las posibles regulaciones del fenómeno de la desinformación en el concreto ámbito electoral deben proteger la integridad de las elecciones, garantizar que sean libres y justas, y que no sean captadas por intereses particulares. Se ha de respetar la libertad de expresión y el valor de la publicidad y propaganda política y su importancia para los procesos democráticos y electorales. Asimismo, ha de respetar el papel de Internet en la esfera pública del discurso político y garantizar que el público tenga acceso a la información legítima necesaria para tomar decisiones de voto autónomas.

Hay que adoptar medidas de seguridad, proteger procesos y personas, convirtiendo las elecciones en una prioridad de seguridad nacional, y las infraestructuras electorales en una infraestructura crítica, dotándola de especial protección.

Hay que adoptar medidas de seguridad, proteger procesos y personas, convirtiendo las elecciones en una prioridad de seguridad nacional, y las infraestructuras electorales en una infraestructura crítica, dotándola de especial protección.

La amenaza más fuerte para la democracia se encuentra en las campañas de desinformación, que sólo son realmente eficaces y, por tanto, amenazas potenciales cuando se realizan de manera profesional y con recursos técnicos y humanos, en las que muchos países emplean recursos de manera estable no solo en periodo electoral. Los rasgos principales de estas campañas pasan más por centrarse en patrones de comportamiento (dado el carácter estructural de las amenazas) y en los actores más que en el análisis y la supresión de contenidos (a diferencia de la información errónea o falsa donde el foco se pone en el propio contenido). El verdadero problema es que los actores que están detrás de estas campañas utilizan comportamientos engañosos para ocultar su identidad con el objetivo de hacer que la organización o su actividad parezca digna de confianza, o para evadir los esfuerzos de las plataformas donde implementan dichas campañas.

Afortunadamente son muchas y muy relevantes las acciones emprendidas por las plataformas frente a su explotación maliciosa para la desinformación. Además, tienen las capacidades de detectar los referidos patrones de comportamiento para reaccionar. El Grupo considera positiva la distinción que ya realizan por lo general las plataformas entre medidas de muy alto impacto,

especialmente en periodo electoral, como puede ser el cierre de un perfil o usuario, así como el bloqueo y retirada de contenidos impidiendo el acceso a los mismos a los usuarios. Mientras que hay otras medidas intermedias como las limitaciones objetivas de interactuación o viralidad. Asimismo, hay medidas que pueden resultar particularmente ponderadas y razonables, como los anuncios o advertencias informativas, que permiten el ejercicio de los propios derechos y libertades de la plataforma y estimular el mismo debate y deliberación social.

No hay duda de la importancia de estas medidas y acciones por las plataformas, tampoco de que existe un claro interés público en la transparencia de tales actuaciones, que deben ser conocidas. De igual modo resulta de interés que la regulación aclare las garantías específicas y en su caso los mecanismos de recurso frente a estas acciones, bien frente a las propias plataformas o mecanismos autorregulatorios, bien frente a las autoridades competentes. Estas garantías de transparencia y debido proceso son importantes en cualquier periodo, pero cobran especial intensidad constitucional en periodo electoral. La regulación podría dejar aún más claro que estas autoridades ya pueden llegar a requerir a las plataformas en periodo electoral en relación a las medidas que hayan adoptado en el ejercicio de sus facultades, especialmente a resultas de requerimientos de partidos y candidatos electorales.

La regulación podría dejar aún más claro que estas autoridades ya pueden llegar a requerir a las plataformas en periodo electoral en relación a las medidas que hayan adoptado en el ejercicio de sus facultades, especialmente a resultas de requerimientos de partidos y candidatos electorales.

Cabe dotar a la Junta Electoral Central (JEC) y los tribunales competentes en el ámbito electoral de capacidad de respuesta ante la desinformación, en su caso recursos suficientes. Asimismo, deben expresarse atribuciones claras para adoptar decisiones eficaces y ágiles como requiere el periodo electoral, también en colaboración con las plataformas.

Desde la perspectiva de protección de datos, también sigue resultando de interés la Circular 1/2019 de la Agencia Española de Protección de Datos (BOE, 2019) cuyos lineamientos deben observarse. En este ámbito, y siempre en el marco de los derechos ya reconocidos de protección de datos, pueden valorarse mecanismos para que los usuarios de las plataformas puedan ejercer de manera ágil y efectiva la posibilidad de conocer los perfilados que poseen los canales a través de los que se recibe publicidad (incluidas web y redes sociales) y, en su caso, puedan gestionar dicho perfil de manera práctica.

En la línea de lo también afirmado en el Capítulo 4, es posible que las actuales limitaciones temporales en los últimos días de campaña, puedan fomentar la aparición de desinformación. Además, el masivo incumplimiento de estas prohibiciones en razón del uso de internet y su dudosa utilidad lleva a replantearse el mantenimiento de la jornada de reflexión y prohibición de publicar encuestas.

De igual modo, tal y como subraya en el Capítulo 3, hay que favorecer los esfuerzos educativos para un mayor conocimiento del sistema electoral, particularmente durante la campaña e incluyendo esos contenidos en los espacios masivos de propaganda electoral en medios de comunicación públicos.

El Grupo ha tenido especialmente en cuenta la importancia de la transparencia de las plataformas respecto de la publicidad electoral y apuesta por respuestas armonizadas y coordinadas como las que se impulsan desde la UE. Así, hay que seguir especialmente la propuesta de legislación para garantizar una mayor transparencia en el ámbito del contenido patrocinado en un contexto político de la Comisión Europea de noviembre de 2021. En todo caso, también cabe mencionar la propuesta regulatoria de Irlanda (Department of the Taoiseach, 2019), de noviembre de 2019 (recomendación 3, sobre la regulación de la transparencia de la publicidad política de pago en línea dentro de los períodos electorales). Baste ahora señalar que, siguiendo la propuesta irlandesa, las plataformas en línea que venden espacios de publicidad tienen que comprobar y determinar si un anuncio entra en el ámbito de los fines políticos, en particular a través de mecanismos que exijan a los anunciantes declarar y verificar su intención de publicar anuncios electorales. El vendedor tendría que verificar la identidad del comprador, así como la dirección del mismo.

Es importante la transparencia de las plataformas respecto de la publicidad electoral.

La publicidad política pagada en línea debe ser etiquetada como tal y mostrar claramente cierta información, o un enlace a la información. De manera clara, debe indicar si se ha utilizado sistemas de *microtargeting* o algoritmos de microfocalización; nombre y dirección del anunciante, si se aplicó la segmentación y la descripción del público objetivo/criterios aplicados y si el público objetivo contiene listas de objetivos “parecidos”; el coste de la publicidad - el requisito debe aplicarse tanto a la creación como a la distribución de contenidos; las métricas, es decir, el número de impresiones que el anuncio debería alcanzar y el plazo de ejecución del anuncio. La información debe divulgarse en tiempo real, siempre que resulte razonable y así lo permita el estado de la tecnología.

Algunos fenómenos particulares como los "deepfakes" pueden merecer en el futuro una respuesta regulatoria.

Algunos fenómenos particulares como los "deepfakes" pueden merecer en el futuro una respuesta regulatoria. Afortunadamente las plataformas ya adoptan diversas medidas respecto de este fenómeno. De momento, cabe mencionar la propuesta de Reglamento de Inteligencia artificial de la UE (Comisión Europea, 2021b). Su artículo 52 se limita esencialmente a asegurar la transparencia en el sentido de que la ciudadanía sepa que el vídeo, audio o contenido está generado por mecanismos de inteligencia artificial y que no es verdadero.

Únicamente, a título ilustrativo, cabe mencionar alguna regulación como las leyes AB 602, y AB 730 de California. Se dispone que 60 días antes a las elecciones no se pueden distribuir "contenidos maliciosos capaces de crear sobre cualquier persona razonable una impresión ciertamente diferente a la que hubiese tenido de poder visualizar el contenido original" (*cause a reasonable person to have a fundamentally different understanding or impression of the expressive content than if he or she had seen the unaltered content*). Por su parte, el 18 de abril de 2019, Texas aprobó su ley de *deepfake*, conocida como SB 751.115 que lo define como "un acto relacionado con la creación de un delito por fabricar un video engañoso con la intención de influir en el resultado de una elección". (También Virginia Code Annotated § 18.2-386.2). A la espera de la evolución normativa y la propuesta de la UE, el Grupo de Trabajo no fórmula propuesta regulatoria concreta al respecto.

Derechos de los usuarios ("estatuto jurídico de la ciudadanía frente a la desinformación")

Nuestro actual ordenamiento jurídico reconoce derechos, algunos de ellos de naturaleza de derecho fundamental, que son proyectables especialmente en el ámbito digital y muchos de ellos pueden tener incidencia en el fenómeno de la desinformación. Así sucede especialmente con las libertades informativas como la libertad de expresión y la libertad de emitir y recibir información veraz o el particular derecho de rectificación, los derechos de participación política, los derechos de la personalidad y en particular la protección de datos. Asimismo, el mes de julio de 2021 se adoptó la Carta de Derechos Digitales que, aunque no tiene valor normativo, implica un amplio y actualizado estatuto de derechos digitales.

En clave de desinformación se dan unas premisas de derechos implicados:

1. La desinformación necesita conocer al público objetivo para distribuirse, su éxito depende de lo que nos gusta, lo que nos mueve, lo que nos interesa, etc. Y para ello por lo general quedan implicados los *derechos de la personalidad*: a la intimidad, la protección de datos, y el secreto de las comunicaciones.
2. Es preciso involucrar responsablemente a la sociedad en la detección y freno de la distribución de contenidos dañinos. En

Foto 6: Dos visitantes prueban un modelo nuevo de teléfono en el Mobile World Congress (MWC) de Barcelona, en 2022. EFE/Enric Fontcuberta

la línea de lo expuesto en el Capítulo 3, es preciso insistir en la importancia de la *educación y alfabetización mediática* como una herramienta esencial para generar conciencia, pensamiento crítico, sensibilización y capacitación para detectar y no convertirnos en correa de transmisión de desinformación. Sin duda, es preciso un refuerzo y adaptación en la regulación curricular para incluir temas de alfabetización mediática y pensamiento crítico y el profesorado debe no sólo estar implicado, sino también capacitado para lograrlo.

3. Los fenómenos desinformativos tienen mucho que ver con los ataques informáticos. Es por ello que resulta esencial la *educación en ciberseguridad*. Las herramientas tecnológicas nos permiten proteger nuestra privacidad y elegir nuestros filtros para la información que queremos recibir (lo que es mucho más deseable que un filtrado ordenado por el Estado).

4. Transparencia respecto al control de contenidos online. La transparencia de las medidas contra la desinformación es la garantía esencial. Transparencia de las decisiones y del proceso de toma de decisiones adoptadas tanto por el sector público como por el sector privado, por humanos o por algoritmos (aunque normalmente se trata de una combinación de ambos). Si no son conocidas las medidas se hace prácticamente inviable su control por los usuarios y la ciudadanía. Además, la supervisión humana para la adopción de decisiones finales debe ser parte del proceso. Actualmente ya son muchas las obligaciones de transparencia y derecho de acceso, así como en su caso de explicabilidad e intervención humana que pueden exigirse en razón de la protección de datos, así como del acceso a la información pública. No obstante, pese al reconocimiento genérico de estos derechos y obligaciones, se hace preciso delimitar y concretar algunas obligaciones y facultades concretas, así como garantías efectivas para los entornos y contextos donde deben proyectarse en el ámbito de la desinformación.

5. Garantías y derechos con relación a las entidades, procedimientos y recursos para reclamaciones frente a contenidos nocivos o en su caso ilícitos vinculados con los fenómenos desinformativos. De nuevo, estas garantías deben darse frente al ámbito público y las medidas que adopten los poderes públicos frente a la desinformación, así como en su caso autoridades del campo audiovisual, autoridades de control relativas a plataformas, de protección de datos o de transparencia. Y de nuevo, garantías frente a las plataformas, intermediarios o en su caso medios de comunicación. La participación judicial o, en su caso de autoridades auténticamente independientes es especialmente

importante en el ámbito de la lucha contra la desinformación. En el caso de estar implicada la defensa y la seguridad nacional es posible que las garantías deban modularse, no obstante, y en todo caso, deben arbitrarse mecanismos que aseguren el control, aunque sea posterior a las medidas adoptadas.

El legislador español debe reforzar y complementar mecanismos de garantía enunciados en la DSA. Se ha de dar una efectiva colaboración público – privada en la que las empresas sirvan de canales directos de comunicación en reclamaciones y la adopción de medidas cautelares, colaborando con la autoridad competente. La plataforma o los proveedores de servicio pueden contribuir con la adopción de medidas de "etiquetado" de la información, reporte de perfiles, sistemas de denuncia para los usuarios y, muy especialmente, criterios claros sobre la carga de la prueba, por ejemplo, ante la imputación de hechos a una persona, que el que emite la información sea quien deba poder probar que son ciertos, ante la exigencia del interesado (*p.ej. *Wikipedia*).

El legislador español debe reforzar y complementar mecanismos de garantía enunciados en la DSA.

6. Las facultades de las plataformas para controlar contenidos nocivos o ilegales pueden pasar por el uso de sistemas de algoritmos, que no puede ser impuesto por los poderes públicos. No obstante, debe existir transparencia sobre su uso tanto respecto de los usuarios y la sociedad civil para que haya rendición de cuentas y, en su caso, control. El monitoreo público o privado de los contenidos no puede afectar al secreto de las comunicaciones en las que haya una razonable expectativa de confidencialidad.

Específicas para la libertad de información:

7. Procedimientos ágiles, sencillos y gratuitos para el ejercicio del derecho de rectificación. Especial consideración a las plataformas de redes sociales (RRSS), y la distinción entre usuarios personas físicas/jurídicas.
8. Criterios claros de responsabilidad cuando el emisor tiene una audiencia claramente significativa como los *influencers* verificados, cargos públicos (debate electoral), profesionales que trabajan para un medio de comunicación social (TV, radio, prensa), *fact-checkers*, y empresas bajo la Ley 34/2002, de 11 de julio, de servicios de la

sociedad de la información y de comercio electrónico (LSSI) para ofrecer confianza, mejor identificar empresas que personas.

9. Visibilización de medios legalmente responsables, aquellos que se rigen por la LSSI o cualesquiera otras normas que exigen una actividad "legal". De este modo se legitima, reconoce y protege el periodismo como profesión, frente al "intrusismo" que desprestigia su credibilidad.

MEDIOS, VERIFICADORES Y PLATAFORMAS Y FENÓMENOS AUTORREGULATORIOS

La desinformación tiene efectos sociales y políticos (Zimmermann y Kohring, 2020) bien documentados, por ejemplo, en la disminución de la confianza en los medios de comunicación o en el aumento de la fidelidad a un gobierno que nos sea ideológicamente próximo (Ognyanova et al., 2020), así como en un aumento de la polarización (Au et al., 2021). Sin embargo, nuestro entendimiento de cómo fluye la desinformación en línea y de cómo combatirla de forma más efectiva tiene aún mucho que mejorar, particularmente en el ámbito de algunas plataformas digitales y muy especialmente en idiomas diferentes al inglés (US Senate Committee on Commerce, Science, & Transportation, 2021). Es importante pues reforzar la investigación en estos ámbitos, lo cual va a requerir también un incremento de la transparencia de las plataformas. Debería abrirse la discusión acerca de la relación entre medios "tradicionales" y las plataformas. ¿Existe la posibilidad de una colaboración más estrecha en la difusión de información de calidad? Hay que insistir en la importancia de la colaboración con instituciones de *fact-checking*.

Es importante la colaboración con instituciones de *fact-checking.*

Y no puede obviarse el impacto directo o indirecto que puede tener la DSA en este debate. En la actual propuesta hay previsiones en materia de "riesgos sistémicos" que van a introducir nuevas obligaciones para las plataformas, algunas de ellas vinculadas precisamente a la evitación de determinadas formas de desinformación.

Protección y defensa del periodismo

Para cumplir con sus responsabilidades de autocontrol ético y garantizar informaciones veraces y plurales en el complejo y nuevo panorama informativo actual digital de convergencia entre prensa, audiovisual e internet es imprescindible la formación y el apoyo de los periodistas como profesionales de la información ante los nuevos retos de la sociedad digital.

El Informe final del Grupo de Expertos de Alto Nivel sobre noticias falsas y desinformación en línea de la UE de 2018 mantiene como ideas fuerza la potenciación de la transparencia del ecosistema de la información, incluyendo a los medios periodísticos, asimismo se afirma la necesidad de salvaguardar la diversidad y la sostenibilidad del ecosistema europeo de medios de comunicación. Igualmente, y relacionado con la defensa y promoción del periodismo se apuesta por desarrollar herramientas para empoderar a los usuarios y periodistas para hacer frente a la desinformación y fomentar un compromiso positivo con las tecnologías de la información en rápida evolución. Como el Plan de Acción para la Democracia Europea recuerda, "los medios de comunicación independientes desempeñan un papel importante en la lucha contra la desinformación y la manipulación del debate democrático". En esta misma línea, hay que tener en cuenta la más reciente recomendación de la Comisión Europea de septiembre de 2021 sobre la protección, la seguridad y la capacitación de los periodistas (Comisión Europea, 2021c).

Este grupo de trabajo comparte estos puntos de partida. El principio básico de la ética del periodismo es garantizar informaciones veraces y plurales a los ciudadanos para que la sociedad de la información sea sociedad del conocimiento de la realidad. Hay que comenzar garantizando la protección y defensa del periodismo ético en contra de la desinformación partiendo de la defensa del periodismo como profesión garantizando su preparación profesional en el ámbito universitario. Debe partirse del protagonismo de los periodistas y medios de comunicación como principales emisores de la información pública, que además del cumplimiento de sus obligaciones jurídicas deben cumplir con principios éticos que se garanticen por Códigos de buenas prácticas y autorregulación.

Debe partirse del protagonismo de los periodistas y medios de comunicación como principales emisores de la información pública.

En este ámbito es un referente ineludible la Resolución sobre la ética del periodismo del Consejo de Europa (1993), conocida como Código Europeo del Periodismo, aprobado en Estrasburgo el 1 de julio de 1993. La ética pública del periodismo para tener efectos prácticos debe aplicarse a través de códigos deontológicos basados en auténtica autorregulación ética para lo que deben reunir los tres requisitos establecidos por el Código de Deontología del Periodismo del Consejo de Europa: en primer lugar, que los principios éticos sean asumidos individual, voluntariamente y en su conjunto por los periodistas-asociaciones profesionales y en su caso por los editores-propietarios de los medios (la ética nunca debe imponerse a diferencia del derecho), que además los harán públicos ante los receptores de la información, los ciudadanos, con el compromiso también de su cumplimiento. En segundo lugar, que este compromiso se someta voluntariamente a la Resolución de comisiones de quejas y deontología autónomas independientes y exteriores a los propios medios de comunicación, aunque nacen por decisión de los propios periodistas-asociaciones profesionales, que recibirán las quejas de los ciudadanos y actuarán también de oficio. En tercer lugar, que en caso de incumplimiento se asuman las consecuencias de la Resolución que como mínimo consistirá en aceptar la publicación de las propias Resoluciones para que los receptores-ciudadanos conozcan qué medio o periodista es ético y cuál no a todos los efectos.

En España hasta el momento la autorregulación ética de los periodistas se ha concretado a través de la FAPE que siguiendo el modelo del Consejo de Europa aprobó en noviembre de 1993 el Código Deontológico actualizado en 2017 con la garantía para su cumplimiento de la Comisión de Arbitraje Quejas y Deontología del Periodismo

Debería garantizarse su continuidad y fortalecimiento y una mayor coordinación con los nueve Colegios de Periodistas de España y especialmente con el de Andalucía y Cataluña dotados de Comisiones de Autocontrol.

Fact-checkers, autorregulación y regulación

Las organizaciones independientes de verificación o *fact-checkers* se han convertido en los últimos años en un actor muy importante en la lucha contra la desinformación. Su labor analizando y desmintiendo la desinformación en su forma más concreta y final contribuye a fomentar un ecosistema informativo donde la mentira es menos viral y menos convincente, como avalan investigaciones académicas (Hameleers y van der Meer, 2020; Porter et al., 2018).

Para ser efectivas esas organizaciones y contar con la necesaria legitimación social han de tener un plus de transparencia respecto al resto de medios de comunicación. En opinión de este Grupo, es especialmente valiosa la experiencia de autorregulación del Código de Principios de la International Fact-checking Network (IFCN), que exige y evalúa periódicamente el cumplimiento de una serie de compromisos concretos por parte de las organizaciones que quieren definirse como organizaciones de *fact-checking*, un compromiso con:

- el apartidismo y la equidad,
- la transparencia de las fuentes,
- la transparencia de financiación y organización,
- la transparencia de la metodología. Un compromiso con las correcciones abiertas y honestas.

Un cumplimiento evaluable de esos compromisos excluye a cualquier organización vinculada por ejemplo a un partido político o que se limite a verificar las declaraciones públicas de otro. También permite que los ciudadanos sepan cómo eligen esas organizaciones qué asuntos investigan, en función de qué parámetros objetivos toman esas decisiones, y qué medidas ponen en marcha para evitar en lo posible un sesgo editorial.

Particularmente importante es la exigencia de ser absolutamente transparentes en sus cuentas: que el público sepa cómo se financian, incluyendo si han llegado a acuerdos con plataformas digitales por las que éstas puedan usar sus contenidos para moderar o para otros fines, en qué condiciones se produce esa colaboración y qué medidas existen para salvaguardar la independencia en el trabajo de la organización de *fact-checking*.

Es importante exigir que los *fact-checkers* sean absolutamente transparentes en sus cuentas, para que el público sepa cómo se financian, o si han llegado a acuerdos con plataformas digitales.

Cada año, las organizaciones de verificación que se adhieren a ese código pasan una evaluación llevada a cabo por un asesor independiente, habitualmente un investigador académico, y esa evaluación es votada por un Consejo Asesor formado por voces autorizadas de entre los verificadores a nivel mundial.

Más allá de esas garantías, la propia naturaleza del trabajo de las organizaciones independientes de *fact-checking* se basa en que no se verifican opiniones, porque tal cosa es imposible. Como su propio nombre en inglés indica, un verificador comprueba "hechos" y puede, conforme a su libertad de expresión y metodología, decir que una opinión se basa en una falsedad, pero no verifica la opinión en sí.

En opinión de este grupo de trabajo, es recomendable que los medios de comunicación que se denominen *fact-checkers* u organizaciones independientes de verificación declaren explícitamente en sus publicaciones si están o no sujetos a códigos de autorregulación como el mencionado de la International Fact-checking Network.

Asimismo, en el caso de que se trate de medios de comunicación públicos que realicen esta labor de verificación, habrán de darse especiales cautelas en su labor de verificación, en particular en periodo electoral y con relación al debate político.

En España se ha llegado a dar alguna proposición de ley de regulación[8] de la actividad de verificación. Los elementos que han sido expuestos pueden ser la base de una posible regulación de la materia.

Habrán de darse especiales cautelas cuando se trate de medios de comunicación públicos que realicen labores de verificación, en particular, en periodo electoral y con relación al debate político.

[8] Proposición de Ley Orgánica de regulación parcial de la verificación de noticias falsas en redes sociales, blogs, sitios web en general y medios de comunicación impresos, digitales y audiovisuales (Boletín Oficial de las Cortes Generales, 2020).

Códigos de buenas prácticas y autorregulación y elementos mínimos o básicos a seguir

Es evidente que la cuestión de la desinformación especialmente en las plataformas y redes sociales merece una atención especial y en buena medida su regulación pasa por fenómenos autorregulatorios o corregulatorios. Los códigos de buenas prácticas y autorregulación deben enmarcarse en el ámbito de la ética y sus principios, que es perfectamente compatible como complemento imprescindible de la prioridad jurídica. El Derecho no puede ni debe regular todas las actividades en todos los ámbitos, ya que impediría la necesaria libertad indispensable tanto de la ciudadanía, así como, y especialmente, de los medios de comunicación, redes, intermediarios y plataformas.

La experiencia, en nuestro país y la Unión Europea, ha acreditado que la autorregulación, cuando se basa en códigos de conducta con compromisos adecuados, es representativa y cuenta con mecanismos eficaces e independientes para su monitorización, puede ser un complemento de la regulación y de los compromisos internos asumidos por las empresas para implementar políticas y estándares de responsabilidad.

Numerosa legislación nacional y europea apuesta por estos modelos que combinan herramientas normativas y de aplicación tanto de la autorregulación, cuando está reconocida, como de la regulación. A nivel europeo se cuenta ya con un código, en este ámbito, que suma los compromisos individuales adoptados por cada una de las principales plataformas. La Comisión Europea ha declarado que espera más esfuerzos y una adhesión amplia a unos estándares comunes, aunque es importante destacar que la propia Comisión ha señalado también que la naturaleza autorregulatoria del código es también una de las limitaciones más importantes a su efectividad (Comisión Europea, 2020c). El código de conducta de la UE, que se ha demostrado una herramienta útil en la lucha contra la desinformación, se encuentra bajo revisión para ser reforzado en estos momentos.

En cualquier caso, los mecanismos de autorregulación a los que ya se ha hecho referencia deben ser tomados con cierta cautela con base a las siguientes consideraciones:

- En España, salvo casos aislados, como el del sector de la publicidad[9], lo cierto es que las experiencias en este terreno han sido siempre

[9] Véase la experiencia de Autocontrol en https://www.autocontrol.es/autorregulacion-publicitaria/

deficientes, especialmente en el terreno de la comunicación audiovisual.

- Son también poco satisfactorias las experiencias de "regulación interna" en los que un determinado medio de comunicación haya articulado mecanismos eficientes de implementación y verificación de una serie de normas o criterios éticos.
- Existe también una tendencia a la fragmentación de la autorregulación, salvo en el sector publicitario ya mencionado, no existiendo pues mecanismos efectivos y asentados de regulación de los medios de comunicación y periodismo en su conjunto (incluyendo nuevos formatos como blogs, *influencers*, etc.)
- Cualquier discusión sobre esta materia debe evitar una definición "corporativa" del concepto de periodismo y abrazar los estándares internacionales en lo que se refiere a la ausencia de autorización o certificación alguna por parte del Estado.

Según se ha señalado, desde 2018 se cuenta con el Código de buenas prácticas de la Unión en materia de desinformación en proceso de revisión y abierto a nuevos participantes. Tal y como se ha adelantado respecto de las propuestas regulatorias el grupo recomienda que toda propuesta de autorregulación en materia de desinformación debe llevarse a cabo en el marco de la UE con el fin de evitar fragmentación y desarmonización y asegurar la unidad de acción y consistencia en toda la UE frente a un fenómeno de naturaleza eminentemente trasnacional.

Toda propuesta de autorregulación en materia de desinformación debe llevarse a cabo en el marco de la UE con el fin de evitar fragmentación y desarmonización.

Asimismo, se recomienda que el proceso actual de revisión del código europeo sobre desinformación incorpore informes de transparencia específicos sobre nuestro país, así como informes sobre las operaciones de información/ influencia con impacto en España.

Además, de cara a los esfuerzos actuales en la revisión del código de conducta sobre desinformación de la UE para medios o plataformas, en los que participa España, este Grupo apunta los elementos que habrían de seguirse a saber:

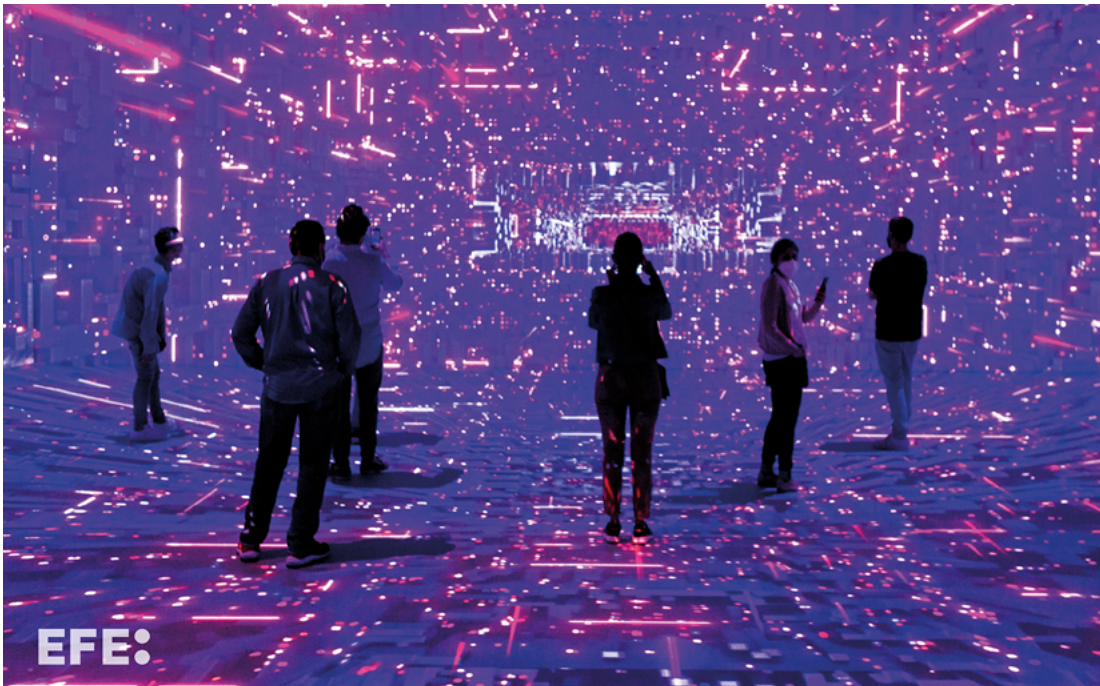
- Su elaboración debería realizarse en consulta con los sectores concernidos y representantes de las entidades de verificación y de la sociedad y usuarios de los contenidos.

- Su contenido y los mecanismos de aplicación que prevean deberán asegurar el cumplimiento de las previsiones que se establezcan en la DSA. De acuerdo con el modelo propuesto en la DSA, deberán contar con un ADR (*Alternative Dispute Resolution Body*) reconocido para resolver las eventuales reclamaciones que se pudieran producir contra las decisiones - de supresión o no de contenidos y/o perfiles- adoptadas por las plataformas o medios que superen el volumen que se establezca finalmente en la DSA para la determinación de los operadores de especial relevancia. Todo ello, sin menoscabo del recurso a los Tribunales de Justicia.
- Debería establecerse una comisión de seguimiento del código europeo con participación de los adheridos y representativa. Periódicamente, debería someterse a evaluación su rendimiento.
- Los códigos o los sistemas de autorregulación serán transparentes respecto de las medidas que se adoptan voluntariamente relativas al fenómeno de la desinformación. En particular detallarán información sobre los criterios para determinar la existencia de una operación de influencia u otros fenómenos masivos y estructurados de desinformación y las medidas adoptadas.
- Determinarán los sistemas de denuncia de contenidos por usuarios, terceros o interesados vinculados al fenómeno de la desinformación. Se concretará asimismo los mecanismos de comunicación existentes con el responsable del contenido denunciado incluyendo la información relativa a las garantías que cuenta frente a una posible retirada o bloqueo del contenido.
- Determinarán los criterios para comunicar a las autoridades datos e información relativa al fenómeno de las campañas de desinformación detectadas.
- Informarán de las órdenes recibidas por las autoridades respecto del ámbito del artículo 8 DSA en su propuesta inicial vinculadas al ámbito de la desinformación o afines
- Los informes de transparencia incluirán información sobre las órdenes recibidas, la moderación de contenidos, incluyendo mecanismos de recomendación, preferencia o priorización de contenidos o los utilizados en sentido inverso. Se detallarán también las reclamaciones recibidas (art. 9 DSA, en su propuesta inicial).
- Las decisiones adoptadas por los mecanismos de resolución de conflictos podrán ser revisadas por una autoridad independiente y, en todo caso, por una autoridad judicial.

- La autoridad independiente, como el coordinador de servicios digitales que menciona la DSA (ver considerandos 74 y 75) o el Ofcom (regulador de los servicios de comunicaciones previsto en el proyecto de ley de 12 de mayo de 2021 de Reino Unido), habrá de estar designada por una mayoría cualificada de al menos 3/5 del Congreso entre personas de reconocido prestigio profesional o académico o con trayectoria judicial. No se considera oportuno atribuir a los consejos audiovisuales existentes las facultades de revisión.

El fenómeno de la desinformación es extremadamente complejo y por ello se recomienda incluir a los servicios de mensajería privada en los mecanismos de autorregulación europeo que se establezcan para dar respuesta a la desinformación. De hecho, las mismas ya implementan mecanismos, protocolos de actuación y políticas con sus usuarios, relacionadas con la desinformación, por ejemplo, informando a los usuarios cuando un mensaje ha sido reenviado o altamente reenviado, así como medidas dirigidas a evitar la viralización de contenidos. La inserción en los mecanismos de autorregulación contra la desinformación de la UE han de potenciar la transparencia y las garantías de los derechos de los usuarios, prestando especial atención a las profundas diferencias entre los servicios de mensajería privada y las redes sociales y plataformas digitales en cuanto a su diseño, uso y expectativas de privacidad de los usuarios. Obviamente, el secreto de las comunicaciones y las expectativas razonables de privacidad de los usuarios, así como el cifrado extremo a extremo y la privacidad y seguridad que proporciona no deben quedar afectados.

Foto 7: Espacio Cloud City del Mobile World Congress (MWC) de Barcelona, en 2021. EFE/Enric Fontcuberta



REFERENCIAS BIBLIOGRÁFICAS

Au, C.H., Ho, K.K.W., y Chiu, D.K. (2021). The Role of Online Misinformation and Fake News in Ideological Polarization: Barriers, Catalysts, and Implications. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-021-10133-9

Boletín Oficial de las Cortes Generales. (2020). *Proposición de Ley Orgánica de regulación parcial de la verificación de noticias falsas en redes sociales, blogs, sitios web en general y medios de comunicación impresos, digitales y audiovisuales* (Serie B, Núm. 95-1, de 17 de julio de 2020). https://www.congreso.es/public_oficiales/L14/CONG/BOCG/B/BOCG-14-B-95-1.PDF

Boletín Oficial del Estado. (2019). *Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General* (BOE núm. 60, de 11 de marzo de 2019). https://www.aepd.es/es/documento/boe-2019-3423.pdf

Boletín Oficial del Estado. (2020). *Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobada por el Consejo de Seguridad Nacional* (BOE núm. 292, de 5 de noviembre de 2020, 96673-96680). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-13663

Comisión Europea. (2018). *Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

Comisión Europea. (2020). *Plan de Acción para la Democracia Europea* (COM(2020) 790 final). https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0790&from=ES

Comisión Europea. (2020b). *Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica*

la Directiva 2000/31/CE (COM(2020) 825 final). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020PC0825&from=en

Comisión Europea. (2020c). *Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement* (SWD(2020) 180 final). https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement

Comisión Europea. (2021). *Orientaciones de la Comisión Europea sobre el refuerzo del Código de Buenas Prácticas en materia de Desinformación* (COM(2021) 262 final). https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021DC0262&from=EN

Comisión Europea. (2021b). *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la unión* (COM(2021) 206 final). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0206

Comisión Europea. (2021c). Sobre la g*arantía de la protección, la seguridad y el empoderamiento de los periodistas y los otros profesionales de los medios de comunicación en la Unión Europea* (RECOMENDACIÓN (UE) 2021/1534). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32021H1534

Comisión Europea. (2021d). Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre la transparencia y la segmentación de la publicidad política (COM(2021) 731 final, 2021/0381 (COD)).https://eur-lex.europa.eu/resource.html?uri=cellar:9cec62db-4dcb-11ec-91ac-01aa75ed71a1.0015.02/DOC_1&format=PDF

Comisión Europea. (2021e). ANEXOS a la propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre la transparencia y la segmentación de la publicidad política (COM(2021) 731 final). https://eur-lex.europa.eu/resource.html?uri=cellar:9cec62db-4dcb-11ec-91ac-01aa75ed71a1.0015.02/DOC_2&format=PDF

Consejo de Europa. (1993). *Código Europeo de Deontología del Periodismo* (Resolución 1003). http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16414

Department of the Taoiseach. (2019). *Online Political Advertising in Ireland: Regulation of Transparency*. https://www.gov.ie/en/policy-information/7a3a7b-overview-regulation-of-transparency-of-online-political-advertising-/#

Hameleers, M. y van der Meer, T.G.L.A. (2020). Misinformation and polarization in a high-choice media environment: How effective are political fact-checkers? *Communication Research*, 47(2), 227-250. https://journals.sagepub.com/doi/pdf/10.1177/0093650218819671

Library Of Congress. (2019). *Government Responses to Disinformation on Social Media Platforms*. https://www.loc.gov/item/2019713404/

Library Of Congress. (2019b). *Initiatives to Counter Fake News in Selected Countries*. https://www.loc.gov/item/2019668145/

Naciones Unidas. (2021). *La desinformación y la libertad de opinión y de expresión* (A/HRC/47/25). https://www.ohchr.org/es/documents/reports/disinformation-and-freedom-opinion-and-expression-report-special-rapporteur

Ognyanova, K., Lazer, D., Robertson, R.E., y Wilson, C. (2020). Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. *Harvard Kennedy School (HKS) Misinformation Review*, 1(4). https://doi.org/10.37016/mr-2020-024

Porter, E., Wood, T. J., y Kirby, D. (2018). Sex trafficking, Russian infiltration, birth certificates, and pedophilia: A survey experiment correcting fake news. *Journal of Experimental Political Science*, 5(2), 159-164. https://doi.org/10.1017/XPS.2017.32

US Senate Committee on Commerce, Science, & Transportation. (2021). *Protecting Kids Online: Testimony from a Facebook Whistleblower*. https://www.commerce.senate.gov/2021/10/protecting%20kids%20online:%20testimony%20from%20a%20facebook%20whistleblower

Zimmermann, F. y Kohring, M. (2020). Mistrust, disinforming news, and vote choice: A panel survey on the origins and consequences of believing disinformation in the 2017 German parliamentary election. *Political Communication*, 37(2), 215-237. https://doi.org/10.1080/10584609.2019.1686095

ANEXO: INFORMACIÓN REMITIDA POR FACEBOOK, GOOGLE Y TWITTER SOBRE ESTRATEGIAS Y ACTIVIDADES PARA COMBATIR LA DESINFORMACIÓN

El papel del sector privado: Estrategia de Facebook para luchar contra la desinformación

Luchar contra la desinformación, proteger la integridad de las elecciones al tiempo que se preserva la libertad de expresión es una prioridad absoluta para Facebook. Aprovechando las lecciones del pasado y las aportaciones de expertos y responsables políticos de todo el espectro político, hemos realizado importantes inversiones en equipos y tecnologías para mejorar la seguridad de las elecciones y las estamos desplegando allí donde tendrán el mayor impacto. Hemos participado en más de 200 elecciones en todo el mundo desde 2017, y hemos creado nuevos productos y desarrollado políticas más sólidas para ayudarnos a prepararnos para futuras elecciones.

Tenemos más de 35.000 personas trabajando en seguridad en todo el mundo. Su trabajo consiste en vigilar la actividad sospechosa, identificar rápidamente los contenidos y comportamientos que infringen nuestras políticas, eliminarlos y evitar que se vuelvan a utilizar. Tenemos 40 equipos involucrados en este trabajo, con más de 500 personas dedicadas exclusivamente a las elecciones. Nuestra estrategia para proteger las elecciones no sólo se aplica durante los momentos críticos, sino durante todo el año, y se centra en tres áreas:

- Eliminar los contenidos perjudiciales y reducir la desinformación
- Impedir las injerencias
- Aumentar la transparencia y el control de los usuarios

Nota preliminar sobre la terminología

En el debate sobre la desinformación hay mucha confusión entre conceptos como desinformación, información falsa o errónea, injerencia extranjera, operaciones de influencia/información e incluso integridad electoral.

En Facebook, utilizamos el término desinformación para referirnos a las afirmaciones que son engañosas o falsas. Por otro lado, utilizamos el término operaciones de influencia (OI) para describir las acciones coordinadas que tienen como objetivo manipular o corromper el debate público con un objetivo estratégico. Dos indicadores clave de las OI son la inautenticidad y la coordinación.

La distinción entre desinformación y OI es importante, porque las preocupaciones políticas que subyacen a cada una de ellas son diferentes, y la respuesta más adecuada de plataformas como Facebook también será diferente. Una diferencia fundamental en la forma de abordar la desinformación y las OI es que distinguimos entre ambas en función del actor/comportamiento y del contenido. En el caso de las OI, nos centramos en los actores y su comportamiento, mientras que en el caso de la desinformación nos centramos en el contenido.

Eliminar contenidos perjudiciales y reducir la desinformación

Aplicamos una estrategia basada en tres pilares -eliminar, reducir e informar- para abordar el contenido problemático en toda la familia de aplicaciones de Facebook. Esto implica eliminar el contenido que infringe nuestras políticas, reducir la difusión del contenido problemático que no infringe nuestras políticas pero que aun así socava la autenticidad de la plataforma, e informar a las personas con información adicional para que puedan elegir dónde hacer clic, qué leer o compartir.

Asimismo, estamos comprometidos con esfuerzos de autorregulación que abarcan los tres elementos de esta estrategia, como el Código de Prácticas de la UE sobre Desinformación. El Código es una herramienta ágil y novedosa que se lanzó de cara a las elecciones al Parlamento Europeo de 2019 y que se ha convertido en un activo en la lucha contra la desinformación COVID-19. En base a las orientaciones de la Comisión Europea (mayo de 2021) estamos trabajando con los demás signatarios en una versión actualizada del Código, reforzada con definiciones, una mayor transparencia y cooperación con las comunidades de investigación y *fact-checking*.

Eliminar

Eliminamos el contenido que viola nuestras Normas de la Comunidad:

- Cuentas falsas y cuentas con comportamientos no auténticos (desactivamos más de un millón de cuentas falsas al día en el momento de su creación).
- La desinformación que pueda contribuir a un riesgo de violencia o daño inminente,
- Fraude o injerencia en el voto, lo que incluye cualquier tergiversación sobre cómo participar en el proceso de votación como las fechas, el lugar, la hora, los métodos y la calificación.
- Anuncios que infrinjan nuestras Políticas de Publicidad, incluidos los anuncios con afirmaciones desacreditadas por *fact-checkers* o, en ciertas circunstancias, por organismos autorizados (como la OMS en el ámbito de la Covid-19), así como nuestras Normas de la Comunidad.

Desde el comienzo de la pandemia, hemos eliminado más de 20 millones de casos de desinformación sobre el COVID-19 en Facebook e Instagram.

Reducir

Para contenido problemático que no incumple nuestras Normas de la Comunidad pero que socava la autenticidad de la plataforma como el *clickbait* y el contenido desacreditado por fact-checkers independientes, reducimos su presencia en la sección de noticias. Para aumentar la transparencia en este trabajo, Facebook lanzó públicamente las Directrices de Distribución de Contenidos (CDG), que explican qué contenido recibe una distribución reducida en Facebook porque es problemático o de baja calidad. Estos criterios y decisiones de clasificación se desarrollaron en colaboración con nuestra comunidad global y de expertos externos.

De esta manera, cuando un contenido es degradado se reduce significativamente el número de personas en Facebook e Instagram que lo ven.

¿Cómo lo hacemos?

Para esta importante tarea, confiamos en nuestra colaboración con *fact-checkers* independientes. Mantenemos una colaboración global con la International Factchecking Network (IFCN) y colaboramos con *fact-checkers* independientes certificados por la IFCN:

- Facebook trabaja con más de 80 organizaciones independientes de fact-checkers en 60 idiomas en todo el mundo para revisar y calificar la precisión del contenido en nuestra plataforma.
- En España colaboramos con EFE Verifica, Newtral, Maldita y AFP, todas ellas acreditadas por la IFCN.

¿Cómo funciona la colaboración en la práctica?

Nuestro enfoque se centra en identificar el contenido que debe ser revisado por los fact-checkers independientes mediante una combinación de:

- Tecnología (*Machine Learning*)
- Denuncias de los usuarios
- Revisión humana
- Los propios *fact-checkers*

A continuación, los *fact-checkers* eligen qué contenido revisar y calificar.

Finalmente, FB actúa sobre el contenido calificado como falso por los *fact-checkers* degradándolo en el *News Feed*. Además, las páginas que compartan repetidamente contenido calificado como falso por los *fact-checkers* verán reducida la distribución de su página en la sección de noticias y se eliminará su capacidad de monetización y publicidad. Hemos ampliado esta política para incluir también sanciones a las cuentas individuales. Asimismo, reducimos la distribución de otros contenidos sensacionalistas y de spam, como el *clickbait* y el *engagement bait*, que también pueden incluir desinformación.

Informar

Ayudamos a prevenir la difusión de desinformación proporcionando contexto adicional y conectando a las personas directamente con información fiable para que puedan tomar decisiones informadas. Estos son algunos ejemplos:

- Etiquetas de desinformación: Aplicamos etiquetas de advertencia y notificaciones en los contenidos verificados como falsos por los f*act-checkers*.
- Añadimos un mensaje de advertencia a las personas que intentan compartir contenidos etiquetados como falsos para que se lo piensen dos veces. Sabemos que cuando se coloca una pantalla de advertencia en una publicación, el 95% de las veces la gente no hace clic para verla.
- Más recientemente, hemos empezado a mostrar mensajes en la sección de noticias para las personas a las que les ha gustado, han reaccionado o han comentado desinformación sobre la COVID-19 antes de que fuera eliminada, y a redirigirles a la página web de la OMS donde se desmienten bulos.
    - Hemos etiquetado y reducido la visibilidad de más de 167 millones de contenidos sobre el COVID-19 tras ser desmentidos por *fact-checker*s independientes.
- Además, informamos a las personas antes de que sigan a una página que ha compartido repetidamente contenido que los *fact-checkers* han calificado como falso.
- Conectamos a la gente con información precisa y autorizada:
    - **Centro de Información COVID-19**. Lanzamos el Centro de Información Covid en Facebook donde se incluyen actualizaciones en tiempo real de las autoridades sanitarias nacionales (Ministerio de Sanidad en España) y de organizaciones mundiales como la OMS, así como artículos, vídeos y publicaciones útiles sobre el distanciamiento social y la prevención de la propagación de la COVID-19. La gente también puede seguir el Centro de Información sobre COVID-19 para recibir actualizaciones de las autoridades sanitarias directamente en su *News Feed*. Hemos conectado a más de 2.000 millones de personas con recursos de las autoridades sanitarias a través de nuestro Centro de Información sobre COVID-19 y de ventanas emergentes educativas en Facebook e

Instagram con más de 600 millones de personas que han hecho clic para obtener más información.

- Hemos lanzado productos, como el registro de votantes y los recordatorios del día de las elecciones, para conectar a las personas con información precisa sobre cuándo y cómo votar. En EE.UU., lanzamos un Centro de Información sobre el Voto en Facebook e Instagram, que sirvió como ventanilla única para dar a los votantes estadounidenses las herramientas y la información que necesitan para hacer oír su voz en las urnas.

- **Contexto adicional sobre el contenido que comparten las personas:** Hemos introducido una nueva pantalla de notificación que permite a los usuarios saber si los artículos de noticias que van a compartir tienen más de 90 días de antigüedad.
- **Alfabetización mediática y digital:** También estamos invirtiendo en iniciativas de alfabetización mediática y digital para concienciar y ayudar a las personas a ser más críticas con la información que reciben. En España lanzamos GeneraZion, un programa educativo sobre seguridad en internet y alfabetización mediática para jóvenes que incluye formaciones en colegios y contenidos educativos interactivos en su plataforma digital. En su segunda edición GeneraZion ha llegado a 15,000 estudiantes en formaciones directas en 200 colegios y a 75.000 más en la plataforma digital.

Prevenir la injerencia/Operaciones de Influencia

Una parte fundamental de nuestra estrategia para prevenir las OI es trabajar con las autoridades gubernamentales, los cuerpos y fuerzas de seguridad, los expertos en seguridad, la sociedad civil y otras empresas tecnológicas para detener las amenazas emergentes, estableciendo una línea de comunicación directa, compartiendo conocimientos e identificando oportunidades de colaboración.

Como se ha mencionado anteriormente en la sección de terminología, la no autenticidad y la coordinación son dos indicadores clave de las OI. Para combatir esta amenaza, hemos desarrollado una política de comportamiento no auténtico que se dirige a los esfuerzos coordinados para manipular el debate público con un objetivo estratégico, donde las cuentas falsas son fundamentales para la operación. Esto nos permite eliminar las redes de cuentas, páginas y grupos basándonos en señales de comportamiento. Hay dos niveles de estas

actividades que trabajamos para detener: 1) el comportamiento inauténtico coordinado en el contexto de campañas nacionales no gubernamentales (CIB) y 2) el comportamiento inauténtico coordinado en nombre de un actor extranjero o gubernamental (FGI).

- Hemos retirado más de 100 redes en todo el mundo por participar en comportamientos inauténticos coordinados (CIB) desde 2017.

Es importante señalar que los actores que participan en OI no tienen por qué utilizar necesariamente la desinformación; la mayoría de los contenidos compartidos en campañas de OI no son probadamente falsos y, de hecho, serían un discurso político aceptable si fueran compartidos por actores auténticos. El verdadero problema es que los actores que están detrás de estas campañas utilizan comportamientos engañosos para ocultar su identidad para hacer que la organización o su actividad parezca digna de confianza, o evadir los esfuerzos de aplicación de nuestras normas.

Aumentar la transparencia y el control de los usuarios

Creemos que una mayor transparencia lleva a una mayor rendición de cuentas. Por este motivo proporcionamos un nivel de transparencia líder en la industria en torno a la publicidad política y las páginas para que las personas pueda ver quién está tratando de influir en ellos. Esto incluye:

- **Anuncios políticos y temáticos:** Los anuncios sobre temas sociales, elecciones o política incluyen avisos de “Pagado por” para mostrar quién está detrás del anuncio.
- **Verificación de los anunciantes políticos:** Para publicar un anuncio político o de temas sociales, los anunciantes deben pasar por nuestro proceso de autorización, que incluye demostrar quiénes son y dónde viven.
- Nuestra **biblioteca de anuncios** ofrece una base de datos de anuncios de acceso público en la que se pueden realizar búsquedas y que permite a periodistas, reguladores, grupos de vigilancia, investigadores, académicos y personas en general exigir responsabilidades a los anunciantes. Para ayudar investigar los anuncios, la biblioteca de anuncios ofrece:
    - Una colección exhaustiva y con capacidad de búsqueda de todos los anuncios actualmente activos (políticos y no

políticos) que se ejecutan en las aplicaciones y servicios de Facebook.

    - Un archivo de anuncios políticos que permanecen en la biblioteca durante 7 años.
    - Información agregada.

- **Transparencia de la página**: En Facebook, mostramos información sobre las páginas, como cuándo se creó, los cambios de nombre y la ubicación de los administradores de la página. También empezaremos a etiquetar los medios de comunicación que creemos que están total o parcialmente bajo el control editorial de su gobierno como medios controlados por el Estado.
- **Información sobre la clasificación de las noticias:** Los usuarios pueden hacer clic en la funcionalidad "¿Por qué estoy viendo esto?" y "¿Por qué estoy viendo este anuncio?" en las publicaciones y anuncios para entender por qué están viendo una noticia o contenido determinado, además de poder controlar lo que ven de sus amigos, páginas y grupos en la sección de noticias. Es la primera vez que incorporamos información sobre el funcionamiento de la clasificación de contenido directamente en la aplicación.

Además de la transparencia, creemos que es importante dar más control a las personas sobre los anuncios que ven, y por eso, en el caso de los anuncios políticos y de temas sociales, hemos introducido recientemente controles para que la gente vea menos anuncios de este tipo en Facebook e Instagram. A través de la herramienta Preferencias de Anuncios, los usuarios pueden desactivar todos los anuncios de temas sociales, electorales o políticos de candidatos, u otras organizaciones que tengan el aviso de exención de responsabilidad política "Pagado por". Hemos lanzado esta opción en Estados Unidos y pretendemos que esté disponible en los países en los que tenemos control sobre los anuncios sobre temas sociales, elecciones y política a finales de este otoño.

Información sobre cómo Google combate la desinformación en diferentes ámbitos[10]

1. **Hacer que la calidad cuente en nuestros sistemas de** clasificación: diseñamos nuestros sistemas de clasificación para que eleven la información fiable y reduzcan la difusión de contenidos de baja calidad en nuestros servicios. Por ejemplo*:*

    - En la Búsqueda de Google, damos más peso a la autoridad que a la relevancia en respuesta a las búsquedas relacionadas con la salud, el sustento o el compromiso cívico de nuestros usuarios (incluidas las búsquedas relacionadas con las noticias). En tiempos de crisis y de noticias de última hora, duplicamos el peso en esa dirección (ya que son momentos en los que los malos actores entran en acción).
    - En YouTube, también trabajamos para elevar los canales con autoridad en respuesta a las búsquedas de los usuarios relacionadas con las noticias, la salud, los medios de vida o temas similares que son propensos a la desinformación, tanto en nuestra página de resultados de búsqueda como en nuestros paneles de "ver a continuación". Además, hemos desarrollado "estantes" de noticias dedicados que elevan los canales de noticias autorizados en los resultados de búsqueda y en la página de inicio de YouTube. Y a principios de 2019, anunciamos cambios en las recomendaciones de YouTube con el fin de reducir la difusión de contenidos límite y de contenidos que podrían desinformar a los usuarios de forma perjudicial, como los vídeos que promueven una falsa cura milagrosa para una enfermedad grave, que afirman que la Tierra es plana o que hacen afirmaciones descaradamente falsas sobre acontecimientos históricos como el 11-S.

2. **Contrarrestar a los actores maliciosos y proteger a nuestros usuarios:** nuestros equipos trabajan duro para impedir que los actores maliciosos abusen de nuestras plataformas y para proteger a nuestros usuarios de la desinformación perjudicial.

    - Para contrarrestar las operaciones de influencia y las campañas de desinformación, contamos con múltiples equipos internos que identifican a los actores maliciosos dondequiera que se

[10] Traducción automatizada del inglés original

originen, desactivan sus cuentas y comparten la información sobre las amenazas con otras empresas y con las fuerzas del orden. Proporcionamos actualizaciones mensuales sobre estas operaciones en nuestro boletín TAG (disponible en el blog TAG). Reforzamos este trabajo durante las elecciones.

- Desarrollamos y aplicamos políticas para reprimir los comportamientos maliciosos y ciertos tipos de desinformación perjudicial.

    - Nuestras políticas en la Búsqueda de Google, Google Noticias, YouTube y nuestros productos publicitarios describen claramente las conductas prohibidas, como la tergiversación de la propiedad o el propósito principal en Google Noticias y nuestros productos publicitarios, o una amplia gama de prácticas engañosas en YouTube.

    - Además, nuestras políticas también prohíben ciertos tipos de información errónea perjudicial: por ejemplo, nuestras políticas de YouTube y de anuncios prohíben los medios de comunicación manipulados de forma engañosa o la información sobre el procedimiento de votación o la elegibilidad de los candidatos que contradiga los registros oficiales del gobierno. YouTube también prohíbe los contenidos que apuntan a un individuo o grupo con teorías conspirativas que se han utilizado para justificar la violencia en el mundo real.

- Además, informamos sobre nuestro trabajo para proteger la integridad electoral. Hemos introducido un Informe de Transparencia de Anuncios Electorales específico para la UE y una biblioteca de anuncios con capacidad de búsqueda para ofrecer más información sobre quién compra anuncios electorales, a quién van dirigidos y cuánto dinero se gasta.

En abril de 2020, para ofrecer aún más transparencia y dotar a los usuarios de más información sobre quién les hace publicidad, empezamos a ampliar la verificación de identidad a todos los anunciantes de nuestras plataformas. Como parte de esta iniciativa, todos los anunciantes deberán completar un programa de verificación para poder comprar anuncios en nuestra red. Los anunciantes tienen que presentar una identificación personal, documentos de constitución de la empresa u otra información que demuestre quiénes son y el país en el que operan. En cuanto a los plazos, el programa de verificación de la

identidad de los anunciantes se extenderá a la UE a partir del primer trimestre de 2021, y a los anunciantes de otras partes del mundo durante el resto de 2021 y más allá.

Este cambio facilita a los usuarios la comprensión de quién es el anunciante que está detrás de los anuncios que ven en Google y les ayuda a tomar decisiones más informadas cuando utilizan nuestros controles publicitarios. También contribuirá a la salud del ecosistema publicitario digital al detectar a los malos actores y limitar sus intentos de tergiversación.

3. **Capacitar a los usuarios con el contexto, la formación y las herramientas de retroalimentación** que pueden ayudarles a detectar y dar su opinión sobre la desinformación en línea.

    - Proporcionamos contexto a los usuarios en el momento en que más importa: cuando están buscando o viendo contenidos:

        - En *las búsquedas*, los paneles de conocimiento ayudan a los usuarios a comprender mejor el tema de sus consultas. También facilitamos la detección de comprobaciones de hechos directamente en los resultados de las búsquedas.

        - En *Google Noticias*, además de las comprobaciones de hechos, nuestra función de Cobertura Completa consiste en proporcionar más contexto a los usuarios sobre un artículo o historia que siguen.

        - En *YouTube*, además de mostrar paneles informativos de *Fact-Check* en los resultados de la búsqueda, proporcionamos contexto a los usuarios en forma de paneles informativos dirigidos a diferentes tipos de contexto, como temas generales y noticias recientes propensas a la desinformación (como el alunizaje), o sobre el hecho de que un canal haya recibido financiación gubernamental o pública.

        - Trabajamos con expertos en alfabetización mediática para ayudar a los consumidores de noticias, especialmente a los adolescentes, a comprender mejor el panorama de las noticias en línea y cómo detectar la desinformación. Google.org se ha comprometido a invertir 10 millones de dólares en todo el mundo para apoyar esta causa,

empezando por una campaña de 3 millones de dólares en Estados Unidos en colaboración con MediaWise, Stanford, Poynter y la LMA.

- Proporcionamos herramientas de retroalimentación que permiten a los usuarios alertarnos cuando nos equivocamos. Son accesibles en la mayoría de las funciones de búsqueda y bajo cada vídeo de YouTube.

Por último, hemos redoblado nuestro trabajo contra la desinformación perjudicial durante la pandemia de COVID-19. Todos los resultados pueden encontrarse en el informe adjunto.

Información sobre cómo Twitter combate la desinformación

Twitter ha permitido que personas de todo el mundo expresen libremente su opinión y ha ampliado su derecho a usar su voz. Creemos en el poder inigualable de la voz del público, de las personas anónimas, y por esta razón ofrecemos a todas las voces una plataforma en la que ser visibles y escuchadas. Twitter ha sido un factor catalizador en la movilización de diversos movimientos sociales, piedras angulares del cambio social. Movimientos que comenzaron con un simple Tweet -como #MeToo, #8M o #BlackLivesMatter- han terminado movilizando al mundo.

El propósito de Twitter de servir a la conversación pública es ahora más crítico que nunca. Mientras el mundo entero se ha enfrentado recientemente a una emergencia de salud pública sin precedentes, las personas están accediendo a nuestro servicio para escuchar a sus líderes, gobiernos y organizaciones internacionales y acceder a la información autorizada que necesitan para protegerse y proteger a sus familias. Nuestro foco está puesto en ayudar a las personas a encontrar información fiable y mantenerlas seguras, permitiéndoles conectar con otros individuos y seguir lo que pasa en el mundo en tiempo real. Trabajamos y buscamos regularmente socios de confianza, incluidas autoridades de salud pública, organizaciones y gobiernos para informarles de nuestro enfoque.

Creemos que las personas que usan Twitter deben tener el contexto adecuado en torno a la información engañosa para poder decidir por sí mismos la veracidad de la información y, al mismo tiempo, evitar la propagación de contenido que pueda provocar daños fuera de línea.

A continuación, detallamos algunas de las medidas que hemos adoptado para proteger y fomentar una conversación pública saludable.

1. **Política relativa a la información engañosa sobre la COVID-19.** En un momento en el que el mundo entero se enfrentaba a una emergencia de salud pública sin precedentes, desde Twitter quisimos informar abiertamente sobre los desafíos a los que nos enfrentamos y las medidas de contingencia que hemos ido implementando para servir a la conversación pública en este momento crítico.

   En el contexto de una pandemia mundial, la información errónea sobre las vacunas presenta un desafío de salud pública importante y creciente,

y todos tenemos un papel que desempeñar. Twitter tiene un papel importante que desempeñar como un lugar para el debate público de buena fe y la discusión sobre estos asuntos críticos de salud pública. Estamos enfocados en mitigar la información engañosa que presenta el mayor daño potencial para la salud y el bienestar de las personas. Bajo nuestra actual política, podemos exigir la eliminación de los Tweets que incluyan información falsa o engañosa sobre la COVID-19[11].

Desde principios de 2021, es posible que etiquetemos o coloquemos una advertencia en los Tweets que presenten rumores sin fundamento, afirmaciones en disputa, así como información incompleta o fuera de contexto sobre las vacunas. Los tweets que están etiquetados bajo esta guía ampliada pueden vincularse a información de salud pública autorizada o las Reglas de Twitter para proporcionar a las personas contexto adicional e información autorizada sobre COVID-19.

Aviso proactivo en la plataforma: En febrero de 2020**,** en colaboración con el Ministerio de Sanidad lanzamos aviso proactivo que dirige a los usuarios a información autorizada por el Ministerio sobre la COVID-19. De esta manera, queremos asegurarnos de que nuestros usuarios tienen acceso a información fidedigna y de fuentes autorizadas cuando busquen #COVID19, #coronavirus #vacuna y otros términos de activación relacionados en Twitter.

2. **Política de integridad cívica**. Twitter juega un papel fundamental en todo el mundo al potenciar la conversación democrática, impulsar la participación cívica, facilitar un debate político significativo y permitir que las personas respondan a los que están en el poder. Pero sabemos que esto no se puede lograr a menos que la integridad de este diálogo crítico en Twitter esté protegida de los intentos, tanto nacionales como extranjeros, de socavarla.

   Creemos que tenemos la responsabilidad de proteger la integridad de esas conversaciones de la interferencia y la manipulación. Por lo tanto, prohibimos los intentos de utilizar nuestros servicios para manipular o interrumpir procesos cívicos, incluso mediante la distribución de información falsa o engañosa sobre los procedimientos o circunstancias relativos a la participación en un proceso cívico. En los casos en que se use información

[11] Algunos ejemplos en https://help.twitter.com/es/rules-and-policies/medical-misinformation-policy

engañosa que no pretenda manipular o interrumpir directamente procesos cívicos, pero que genere confusión respecto de nuestro servicio, podemos etiquetar los Tweets para brindar contexto adicional.

Las consecuencias de incumplir nuestra política de integridad cívica varían según la gravedad y el tipo de incumplimiento, y los antecedentes de incumplimiento de la cuenta infractora. En los casos en que las cuentas incumplan repetidamente esta política, usaremos un sistema de advertencia para determinar si se deben considerar otras acciones de control de cumplimiento. Creemos que este sistema ayuda aún más a reducir la difusión de información errónea potencialmente dañina y engañosa en Twitter, especialmente cuando se trata de incumplimientos graves de nuestras reglas. Ejemplos de las medidas que podemos tomar: Eliminación del Tweet, Modificaciones del perfil, Etiquetas o Bloqueos y suspensión permanente de la cuenta.

También tenemos etiquetas en Twitter para que quede claro cuando interactúas con una cuenta oficial de gobierno o de medios afiliados a un Estado.

Ofrecemos más contexto cuando lo necesitamos. Como parte de nuestras políticas, usamos etiquetas en Twitter para agregar contexto a afirmaciones objetadas o engañosas, y también reducimos la visibilidad de estos Tweets a fin de mitigar posibles daños. Además, a través de nuestra política relativa a los contenidos multimedia falsos y alterados, agregamos etiquetas al contenido que promueve, con la intención de engañar, contenidos multimedia falsos o alterados.

3. Nuestra **Política relativa al spam y la manipulación de la plataforma** establece que no se pueden usar los servicios de Twitter con el propósito de amplificar o suprimir información de forma artificial, ni llevar a cabo acciones que manipulen u obstaculicen la experiencia de los usuarios en Twitter. Queremos que Twitter sea un lugar donde las personas puedan establecer relaciones, encontrar información confiable y expresarse de manera libre y segura. Para que esto sea posible, no permitimos el spam ni ningún otro tipo de manipulación de la plataforma. Manipular la plataforma es usar Twitter para llevar a cabo acciones masivas, de alta intensidad o engañosas que confunden a los usuarios o que obstaculizan su experiencia. Hay muchas formas de manipular la plataforma, y nuestras reglas están destinadas a contrarrestar una gran variedad de comportamientos prohibidos. Aquí podéis encontrar algunos ejemplos.

Además, en septiembre de 2021, anunciamos que estamos probando una función de etiquetado que permitirá que las cuentas automatizadas se identifiquen a sí mismas para que puedas tener una mejor experiencia en Twitter.

4. **Campañas de Alfabetización Mediática.** Además de nuestro trabajo de productos, políticas y cumplimiento en este espacio, también hemos logrado un gran progreso en torno a la alfabetización mediática. Sabemos que ahora más que nunca la gente debería mirar críticamente la información online.

   En asociación con la UNESCO, produjimos el Manual de alfabetización mediática *Enseñar y aprender con Twitter*. Junto a socios locales como PantallasAmigas, Maldita.es, Al fanar o Plan Internacional España, ayudamos a equipar a las generaciones más jóvenes con habilidades de alfabetización mediática, permitiéndoles hacer las preguntas correctas sobre el contenido con el que interactúan en línea y analizar críticamente las noticias y la información con las que interactúan en Twitter. Les brindamos consejos sobre cómo ser conscientes de su ciudadanía digital y su etiqueta, por ejemplo, sea consciente del tono, sea amable y respetuoso, sea positivo.

   Recientemente lanzamos un proyecto piloto llamado “Birdwatch” para probar soluciones basadas en la comunidad para información engañosa y actualmente estamos recopilando datos sobre su uso entre un grupo seleccionado de usuarios. A través de esto, permitimos que un grupo de usuarios preseleccionado, por ahora, solo en los EE. UU., se registren a través de Twitter. Queremos que tanto los expertos como los no expertos escriban notas de *Birdwatch*.

   También trabajamos con socios y expertos de confianza con respecto a diversos mercados para ayudarnos a entender el contexto local, la cultura y matices. Nuestro Consejo de Confianza y Seguridad nos informa sobre las tendencias recientes e importantes en una variedad de temas. El Consejo de Confianza y Seguridad de Twitter es un grupo de organizaciones de expertos independientes de todo el mundo. Juntos, abogan por la seguridad y nos asesoran a medida que desarrollamos nuestros productos, programas y reglas. Las áreas de enfoque incluyen seguridad y acoso en línea, derechos humanos y digitales, prevención del suicidio y salud mental, explotación sexual infantil y deshumanización.

Además, con carácter general, brindamos formación y otorgamos *AdsForGood* (crédito publicitario pro bono) para apoyar los esfuerzos y actividades de la sociedad civil en la plataforma y fomentar la colaboración mutua.

5. **Operaciones de Información.** Siguiendo los principios de transparencia y con el fin de mejorar la comprensión del público sobre las supuestas campañas de influencia no auténticas, Twitter está publicando archivos relativos a Tweets y contenidos multimedia que creemos que provienen de operaciones de información que están vinculadas con ciertos Estados y que han tenido lugar en nuestro servicio. Creemos que Twitter tiene la responsabilidad de proteger la integridad del debate público, incluso a través de la revelación puntual de información sobre los intentos de manipular Twitter para influir en elecciones y otros debates cívicos por parte de entidades que están vinculadas con ciertos Estados, ya sean nacionales o extranjeras. Igualmente, creemos que la comunidad pública y de investigación está mejor informada gracias a la transparencia.

   En octubre de 2018, presentamos el primer archivo del sector sobre operaciones de información extranjeras potenciales observadas en Twitter. Nuestra opinión fundamental es que estas cuentas deberían ser públicas y permitir búsquedas a fin de que miembros del público, gobiernos e investigadores puedan investigar, aprender y desarrollar conocimientos multimedia para el futuro. La transparencia ha sido un componente esencial de la compañía desde el principio. Hemos ampliado considerablemente este conjunto de datos con varias actualizaciones independientes durante los últimos dos años. Somos la única compañía que ofrece este nivel de detalle y transparencia. Por nuestra parte, estamos adquiriendo, desarrollando y creando un enfoque tecnológico impulsado por el personal con la finalidad de hacer frente a las campañas de influencia no auténticas. Esperamos que las divulgaciones holísticas transparentes como esta nos ayuden a adquirir y a desarrollar las defensas y capacidades sociales necesarias para proteger el debate público[12].

6. En 2019, actualizamos nuestra **Política de Contenido de Carácter Político**. Esta política se aplica a los productos publicitarios de pago de Twitter. Twitter prohíbe en todo el mundo la promoción de contenido de

[12] Nuestro archivo de Operaciones de Información está disponible en https://transparency.twitter.com/es_es/reports/information-operations.html

carácter político. Tomamos esta decisión según nuestra creencia de que el alcance de los mensajes políticos se debe ganar, no comprar.

¿Cómo definimos el contenido de carácter político? Como aquel que hace referencia a un candidato, partido político, funcionario gubernamental electo o designado, elección, referéndum, medida sometida a votación, ley, normativa, directiva o fallo judicial. Los anuncios que contengan referencias a contenido de carácter político, incluidas peticiones de votos, solicitudes de apoyo financiero y promoción a favor o en contra de los tipos de contenido de carácter político mencionados anteriormente, quedan prohibidos en virtud de esta política. Tampoco permitiremos anuncios de ningún tipo de parte de candidatos, partidos políticos o funcionarios del gobierno elegidos o designados.

CAPÍTULO 3

LA ALFABETIZACIÓN MEDIÁTICA, HERRAMIENTA CLAVE EN LA LUCHA CONTRA LA DESINFORMACIÓN

Coordinador sociedad civil:

Aurelio Martín González (Federación de Asociaciones de Periodistas de España)

Coordinador institucional:

Secretaría de Estado de Comunicación (Presidencia de Gobierno)

Autores y colaboradores:

Ofelia Tejerina Rodríguez (Asociación de Internautas)

Desirée García Pruñonosa (EFE Verifica)

Ramiro Fuente Jiménez (EFE Verifica)

Mar Iglesias García (Federación de Organismos o Entidades de Radio y Televisión Autonómicos)

Ana Abade Gil (Google)

Stephane Manuel Grueso Lenoir (Maldita.es)

Guillermo Serrano Peña (Meta)

Yolanda Quintana Serrano (Plataforma en Defensa de la Libertad de Información)

Núria de José Gomar (Red de Colegios de Periodistas)

José Ferrer Castro (Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales)

Camino Rojo Torres (Twitter)

Eva Herrero Curiel (Universidad Carlos III)

Francisco Marcos Martín Martín (Universidad de Málaga)

Charo Sádaba Chalezquer (Universidad de Navarra)

Agustín García Matilla (Universidad de Valladolid)

Salvador Gómez García (Universidad de Valladolid)

Belén Puebla Martínez (Universidad Rey Juan Carlos)

Borja Diaz-Merry Rivas y Myriam Redondo Escudero (Verifica RTVE)

DEFINICIÓN DEL ALCANCE Y LOS OBJETIVOS DEL PROYECTO

La complejidad creciente de la sociedad de la información en la que la ciudadanía de los países occidentales se desenvuelve ha generado nuevos retos a los que hay que dar respuesta. Uno de ellos es qué hacer con el constante acceso a contenidos generados por todo tipo de fuentes, oficiales y personales, profesionales y amateurs, bienintencionadas y malintencionadas, que hacen patente la necesidad de formar a usuarios críticos con la información que reciben y consumen.

Expertos en educomunicación llevan años advirtiendo de los peligros de la desinformación y la necesidad de que los medios y los periodistas trabajen para combatirla y no promocionarla (García Matilla, 1999; Pérez Tornero, 2008; Lara, 2019; Aparici y García Marín, 2019). En los últimos años la desinformación ha pasado a convertirse en un problema social de primer orden que interfiere en la salud de las democracias, en la gestión de asuntos de orden público y que puede tener también un impacto negativo en la vida de las personas (Salaverría et al., 2020). Esto se agrava con el factor subjetivo que Wason (1960) denomina "sesgo de confirmación" y que implica que las personas favorecen el consumo de las informaciones que confirman sus propias creencias o prejuicios. Un rasgo que genera un efecto de "cámaras de eco", acentuado en las redes sociales, que añade más urgencia a la lucha contra la desinformación· Se identifica, en definitiva, con la necesidad de dotar a la ciudadanía de recursos y capacidades personales que le permitan hacer frente a sus propios prejuicios en primer lugar, y a las estrategias de desinformación de las que puede ser víctima en último término.

En los últimos años la desinformación ha pasado a convertirse en un problema social de primer orden que interfiere en la salud de las democracias.

La desinformación no es un fenómeno novedoso, aunque sí lo son las dimensiones que ha adquirido en una sociedad digital interconectada. Para

combatirla se conceptualizó la idea de una «alfabetización o literacia mediática» (*media literacy*) que ha sido el término preferido en el mundo anglosajón, y que, más tarde evolucionó hacia el concepto de competencia mediática. Del mismo modo, en el ámbito iberoamericano se ha acuñado el concepto «educomunicación», a partir de la escuela heredera de Paulo Freire y de la comunicación popular, para englobar los territorios de las alfabetizaciones o literacias múltiples en el contexto luso parlante.

El escenario digital ha añadido las habilidades digitales a esta competencia mediática entendida de una manera más integradora y que interpela no solo a la etapa educativa formal, sino a la formación para toda la vida (Kačinová y Sádaba Chalezquer, 2022). Por ello, como reconocían Ferrés y Piscitelli (2012) "la competencia mediática ha de hacer frente […] a esta complejidad, compaginando la potenciación de la cultura participativa con el desarrollo de la capacidad crítica". Esta competencia incluye seis dimensiones para la formación y la capacitación: lenguajes, tecnologías, procesos de interacción, procesos de producción y difusión, ideología y valores y estética. El enfoque educativo es fundamental. La información errónea y la desinformación están demasiado extendidas como para inscribirlas únicamente en un marco de seguridad. Son cuestiones que es mejor vincular sobre todo a la necesidad de mayor alfabetización mediática y digital entre la ciudadanía, que debiera disponer siempre de conocimientos y recursos de verificación (Redondo, 2018, p. 164).

La información errónea y la desinformación están demasiado extendidas como para inscribirlas únicamente en un marco de seguridad.

En este contexto, el objetivo de estas páginas es proporcionar ideas y articular propuestas que, dentro del marco del Plan Integral de Cultura de la Seguridad Nacional, ayuden a poner en marcha acciones y líneas de trabajo con estos objetivos:

- Concienciar a los ciudadanos de la trascendencia para las sociedades democráticas de la disponibilidad y acceso a fuentes de información plurales y veraces.
- Diseñar planes de capacitación para la ciudadanía adaptando las dimensiones de la competencia mediática de manera estable a la educación formal con escenarios de educación formal e informal, prestando una especial atención a públicos más vulnerables.

ANÁLISIS EN LA UNIÓN EUROPEA Y EN ESPAÑA

El impacto de la desinformación en la Unión Europea

Los países miembros de la Unión Europea han reconocido la amenaza que supone la desinformación y sus efectos en contextos electorales y pandémicos. Las elecciones norteamericanas de 2016 y el referéndum para la salida de Reino Unido de la UE (*Brexit*) hicieron saltar las alarmas en las instituciones europeas considerando que la desinformación comprende una evidente amenaza contra los procesos democráticos y de elaboración de políticas, así como contra la protección de la salud, el medio ambiente o la seguridad de los ciudadanos de la UE (Comisión Europea, 2018). Sin embargo, los esfuerzos de la UE por combatir la desinformación se remontan a fechas anteriores a los acontecimientos citados.

En marzo de 2015, el Consejo Europeo invita a la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, Federica Mogherini, a preparar un plan de acción sobre comunicación estratégica para contrarrestar las campañas de desinformación procedentes de fuera de la Unión (Rusia). Esto condujo a la creación de una división de comunicaciones estratégicas (StratCom) y al primero de sus grupos de trabajo en el seno del Servicio Europeo de Acción Exterior (SEAE). Al final de 2017, la Comisión Europea crea un grupo de expertos para asesorar sobre la lucha contra la desinformación. El grupo presenta un informe, en marzo de 2018, que sienta las bases para la comunicación de la Comisión sobre la lucha contra la desinformación en línea (Comisión Europea, 2018). A finales de ese año, y a sugerencia del Consejo Europeo, la Alta Representante y la Comisión, presentó el *Plan de Acción de la Unión Europea contra la desinformación* (en lo sucesivo, Plan de Acción de la UE), que incluye diez acciones específicas basadas en cuatro pilares de actuación (Comisión Europea, 2018):

I. Mejora de la capacidad de las instituciones de la Unión para detectar, analizar y exponer la desinformación.

II. Refuerzo de las respuestas coordinadas y conjuntas a la desinformación.

III. Movilización del sector privado para combatir la desinformación.

IV. Aumento de la sensibilización y la capacidad de respuesta de la sociedad.

De esta forma se consolida el compromiso de la UE para el empoderamiento de la sociedad, en su conjunto, frente a la desinformación. Un reto que se fundamenta, entre otros eventos, de las elecciones al Parlamento Europeo de 2019, una de las campañas electorales más digitales de la historia reciente. Esta campaña electoral se celebró en un contexto sociopolítico tenso y voluble. En él, las redes sociales han resultado ser un instrumento fundamental para que los políticos lleguen a los votantes y para que los grupos que defienden causas particulares organicen a sus partidarios (Comisión Europea, 2020). Las autoridades europeas, conscientes de las posibles interferencias de agentes externos en los comportamientos y las decisiones de la ciudadanía y en la propia estabilidad y credibilidad de las instituciones de la UE, toman una serie de medidas para apoyar la resiliencia en las elecciones[1].

En el marco del Paquete electoral de la Comisión y del Plan de Acción de la UE se abordan los casos de manipulación informativa que afectan a la UE mediante la refutación de declaraciones falsas en entornos comunicativos en línea y sensibilizando al público sobre los retos y riesgos que plantea la desinformación (Comisión Europea, 2020). Se trata de una propuesta sistémica en la que suman esfuerzos las autoridades competentes de los Estados miembros, las organizaciones de la sociedad civil, los periodistas, los verificadores y las plataformas digitales.

A comienzos de 2020, en los albores de la pandemia por la COVID-19, surgió en internet una corriente de informaciones erróneas, desinformación y bulos digitales que la Organización Mundial de la Salud calificó como *infodemia*. Un término acuñado por la OMS para referirse a "una cantidad excesiva de información -en algunos casos correcta, en otros no- que dificulta que las personas encuentren fuentes confiables y orientación fidedigna cuando las necesitan". De esta forma, se identificaba la situación descrita como una amenaza para la salud pública y la revitalización de la economía. En junio de 2020, la Comisión Europea y el Alto Representante de la Unión, Josep Borrell, publicaron una comunicación titulada *La lucha contra la desinformación acerca de la COVID-19: contrastando los datos*, que examinaba las medidas adoptadas en propuestas anteriores y acciones concretas para combatir la desinformación relativa al coronavirus.

A comienzos de 2020, en los albores de la pandemia por la COVID-19, surgió en internet una corriente de informaciones erróneas, desinformación y bulos digitales que la Organización Mundial de la Salud calificó como *infodemia*.

[1] Véase, por ejemplo, la investigación sobre el uso de las interferencias cibernéticas para manipular las elecciones elaborado por el Centro de Excelencia para la Lucha contra las Amenazas Híbridas. https://www.hybridcoe.fi/wpcontent/uploads/2018/10/Strategic-Analysis-2018-8-Past.pdf

Foto 8: Datos del coronavirus en pantallas, por Markus Spiske.

A medida que las vacunas para paliar los efectos del virus se han desarrollado y puesto a disposición de la ciudadanía, se ha difundido a través de las plataformas digitales información errónea sobre su eficacia y efectos secundarios. La creciente expansión e impacto de estas informaciones han obtenido rápida respuesta por parte de las autoridades europeas. Por ejemplo, se ha intensificado el apoyo de la UE a los verificadores de datos y los investigadores, el refuerzo de las capacidades de comunicación estratégica y la mejora de la cooperación con los socios internacionales, garantizando al mismo tiempo la libertad de expresión y la pluralidad (Comisión Europea, 2020b). Todas estas medidas van dirigidas, nuevamente, a aumentar la resiliencia ante el problema de la desinformación en los Estados miembros.

A estas alturas, son numerosas las voces que responsabilizan a la irrupción de las redes sociales en el ecosistema informativo como agentes clave del fenómeno desinformativo. A lo largo de toda la pandemia, la UE ha alentado a las plataformas digitales a contribuir a la lucha contra las noticias falsas y otros intentos de difundir información errónea eliminando los mensajes de odio y falsos. Esta colaboración ha dado lugar al impulso de medidas para luchar

contra los bulos. Por ejemplo, la plataforma TikTok ha introducido el *banner* "know your facts", que advierte a los usuarios de contenidos que no hayan sido validados. Google ha suprimido cuatro canales de YouTube, así como de una cuenta publicitaria, y de la ampliación de su función de búsqueda a todos los Estados miembros de la UE (Comisión Europea, 2020c). Sin embargo, en el informe que evalúa el Código de Buenas Prácticas (Comisión Europea, 2020d) se ponen de relieve algunas deficiencias respecto a la opacidad de las plataformas firmantes en sus políticas contra la desinformación. Věra Jourová, vicepresidenta responsable de Valores y Transparencia, manifestó que "las plataformas deben ser más responsables, tienen que rendir cuentas y deben ser más transparentes. Ha llegado el momento de ir más allá de las medidas de autorregulación" (Comisión Europea, 2020d). Oportunamente, en diciembre de 2020, la Comisión Europea publicó una propuesta de Ley de Servicios Digitales que propone un marco de transparencia y rendición de cuentas para las plataformas online, en respuesta a los riesgos digitales emergentes.

La desinformación en contextos digitales evoluciona de manera constante. Técnicas de propaganda, perfiles y grupos falsos en redes sociales, publicidad engañosa y *clickbait*, *bots* y *trolls*, inteligencia artificial y *deepfakes* son algunas de las técnicas que adoptan las campañas de desinformación para inferir en los comportamientos y decisiones de la ciudadanía (Redondo, 2016; Alaphilippe et al., 2019). En respuesta a este volátil y amenazante contexto, el Consejo Europeo sugiere revisar y actualizar, periódicamente, el Plan de Acción de la UE con objeto de que los grupos de trabajo frenen la amplia gama de agentes involucrados en la propagación de los bulos y el desorden informativo[2].

El Plan de Acción de la UE contiene medidas oportunas y proactivas para combatir la desinformación. Sin embargo, como se indica en el informe *El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada* (Tribunal de Cuentas Europeo, 2021), se requiere coordinación, seguimiento y evaluación respecto a las estrategias, tácticas y tecnologías creadas, en el seno de la UE, para luchar contra la desinformación.

Respecto a la alfabetización mediática, acción específica del pilar IV del Plan de Acción de la UE, la Unión Europea muestra interés por esta área, así queda atestiguado en las numerosas iniciativas y documentos de orientación

[2] La Comisión Europea, para facilitar la comprensión semántica que ha generado el fenómeno, acuñó el concepto "desorden informativo, que comprende: Información errónea o falsa compartida en redes sociales, pero sin intención de provocar perjuicio alguno; Desinformación o falsa información, compartida con la intención de infligir un daño; Mala praxis, cuando una información veraz es compartida con el objetivo de causar daño (Wardle y Derakhshan, 2017).

elaborados por la UE y los Estados miembros (Consejo de la Unión Europea, 2020). Por ejemplo, la UE, para fomentar la sensibilización acerca de la alfabetización mediática entre los Estados miembros, crea la Semana Europea de la Alfabetización Mediática. Sin embargo, esta iniciativa tuvo una acogida muy irregular: casi la mitad del total de iniciativas se organizaron en Francia, mientras que otros países miembros tuvieron una presencia meramente testimonial. La responsabilidad en materia de alfabetización mediática recae, exclusivamente, en los Estados miembros, por lo que resulta esencial desarrollar planes y herramientas comunes a escala europea. Estas iniciativas y recursos deben adaptarse a la diversidad característica de los países miembros, para facilitar la participación de la ciudadanía y el aprendizaje que proporcionan las actuaciones educomunicativas.

Alfabetización mediática recae, exclusivamente, en los Estados miembros, por lo que resulta esencial desarrollar planes y herramientas comunes a escala europea.

Por otra parte, las acciones impulsadas por la UE carecen de "una estrategia de alfabetización mediática que incluya la lucha contra la desinformación" (Tribunal de Cuentas Europeo, 2021) para que la ciudadanía analice y comprenda críticamente a los medios de comunicación en un panorama cambiante. Hoy, más que nunca, "se requieren competencias en alfabetización mediática para participar activamente en la sociedad democrática; permiten que los ciudadanos accedan, comprendan y traten con los medios de comunicación y los alienta a convertirse en agentes políticos" (McDougall et al., 2018). La desinformación es, sin duda, una oportunidad para la alfabetización mediática. Sin embargo, supondría un inconveniente recurrir a la alfabetización mediática como una solución de urgencia. Se debe evitar subestimar la complejidad que supone la propia educación mediática y la implementación de actuaciones de este tipo (Buckingham, 2019).

La importancia de la alfabetización mediática en el aula tendría como fin que los estudiantes desarrollen, entre otras cosas, "un metalenguaje, una forma de discurso crítico, con el que estarán en condiciones de describir y analizar los acontecimientos en curso" (Buckingham, 2005, p. 267). En definitiva, contribuir a que los estudiantes se conviertan en ciudadanos críticos dentro de un mundo globalizado, complejo y en continua transformación tecnológica soluciona un problema ya existente, en todo caso se trata de una propuesta, dentro de un enfoque holístico, que aporta una solución para tratar de impedir que avance la problemática asociada a la desinformación y los bulos.

La desinformación en la sociedad española: estado de la cuestión

En pleno proceso de recuperación económica e incertidumbre sanitara, la pandemia por la COVID-19 sigue generando una enorme demanda informativa. Sin embargo, en la búsqueda de certezas, la ciudadanía española se encuentra con mensajes confusos, informaciones manipuladas y saturación informativa. Un estudio realizado por el *Reuters Institute for the Study of Journalism*, en colaboración con la Universidad de Navarra, reveló que la mayoría de los españoles reconoce haber estado expuesto a bulos sobre el coronavirus y asuntos políticos (Amoedo et al., 2021). Esta situación encuentra respuesta en las campañas de desinformación que sobre el coronavirus y las decisiones políticas han circulado en redes sociales y sistemas de mensajería instantánea.

En la búsqueda de certezas, la ciudadanía española se encuentra con mensajes confusos, informaciones manipuladas y saturación informativa.

La ciudadanía, objetivo principal de las campañas desinformativas, muestra su vulnerabilidad frente a la rápida transformación y el refinamiento de las diferentes herramientas y procedimientos de cibercomunicación que se ponen en marcha para causar el caos y la confusión (Centro Criptológico Nacional [CCN], 2019). Según se desprende de la encuesta realizada por la consultora *Ipsos Global Advisor* (IPSOS, 2018), España es el país europeo que muestra una actitud más ingenua frente a los bulos. El 57% de los españoles admite haber creído alguna vez como verdadera la información de una noticia falsa.

El 57% de los españoles admite haber creído alguna vez como verdadera la información de una noticia falsa.

La "bancarrota informativa" también ha quebrado la confianza de la ciudadanía española, principalmente, en los medios de comunicación y el Estado. En este sentido, el informe *Trust Barometer Spain 2021* muestra que "la mayoría de encuestados cree que tanto los medios de comunicación (69%) como el Gobierno (65%) intentan confundir a los ciudadanos" (ELDELMAN, 2021), de manera premeditada difundiendo datos e informaciones falsas. En este clima de desinformación y desconfianza han proliferado iniciativas gubernamentales, no gubernamentales, académicas y periodísticas para luchar contra los daños ocasionados por el fenómeno desinformativo.

El Gobierno de España, tomando como punto de partida el Plan de Acción contra la Desinformación de la UE y el Plan de Acción para la Democracia Europea, ha adoptado su propia estrategia nacional frente a la desinformación. La estrategia establecida por el Gobierno tiene como fin prevenir, detectar y responder a las campañas desinformativas que pretendan menoscabar los intereses nacionales o los procesos electorales (Boletín Oficial del Estado [BOE], 2019). Los órganos y organismos que forman parte del Sistema de Seguridad Nacional en esta materia son el Consejo de Seguridad Nacional, el Comité de Situación, la Comisión Permanente contra la desinformación, las demás Autoridades públicas competentes, el sector privado y la sociedad civil.

La inclusión del sector privado y la sociedad civil en el Sistema de Seguridad Nacional supone la consolidación de un cambio de paradigma en la lucha contra la desinformación. Para reducir el desfase entre el conocimiento de las estrategias desinformativas y las acciones contra las mismas, se establece un modelo de gestión colaborativa que pretende facilitar una mayor participación social y privada con la que complementar las medidas gubernamentales (Arteaga, 2020).

La inclusión del sector privado y la sociedad civil en el Sistema de Seguridad Nacional supone la consolidación de un cambio de paradigma en la lucha contra la desinformación.

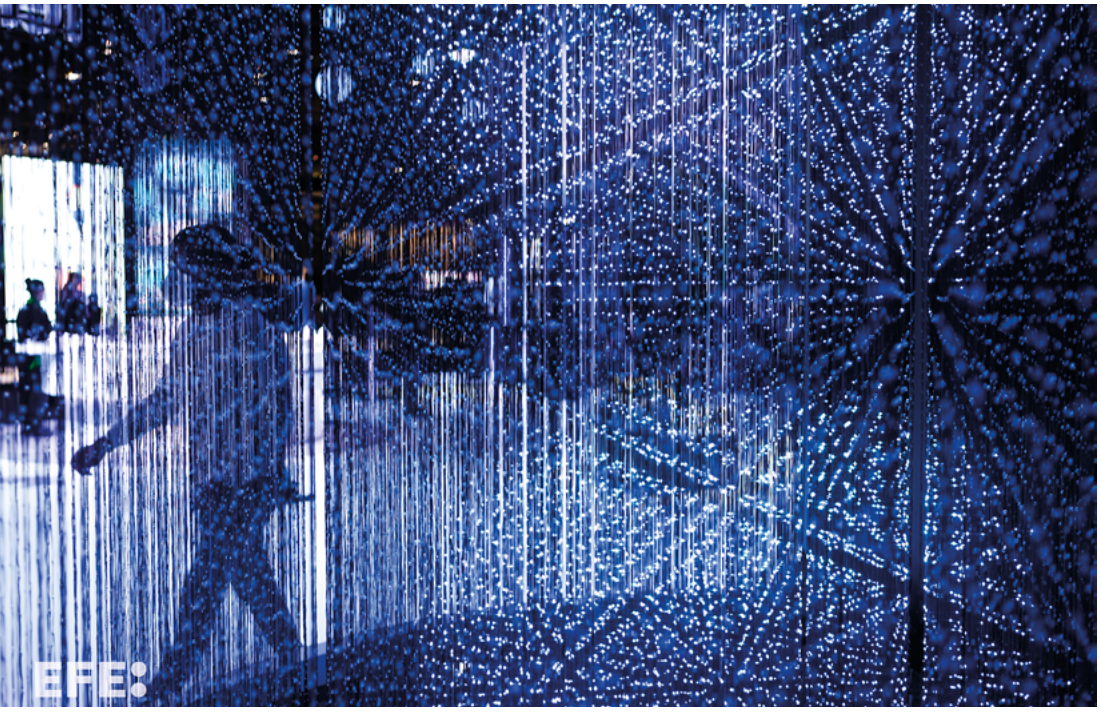
Destinada a impulsar el desarrollo de una resiliencia social ante las acciones de desinformación y a difundir informes de buenas prácticas, el Centro Criptológico Nacional (CCN) crea, en 2020, una sección dedicada a la desinformación. En la sección se han incluido recursos y materiales para empoderar a la ciudadanía. La primera medida tomada por el CCN ha sido la publicación de un informe de buenas prácticas titulado *Desinformación en el ciberespacio* (CCN, 2019). El objetivo de esta guía es "explicar las principales características y metodología de las actuales acciones de desinformación"; y un protocolo para que la ciudadanía y los usuarios finales de medios de comunicación digital "dispongan de las herramientas que les permitan consumir y compartir información de manera crítica y evitar ser cómplices involuntarios de acciones ofensivas contra los intereses del Estado" (CCN, 2019, p. 8).

Paralelamente, se constituye el Foro Nacional de Ciberseguridad, un espacio de colaboración público-privada, para compartir y generar conocimiento a partir de la información, impulsado por el Consejo de Seguridad Nacional, y en donde el CCN y el INCIBE ocupan las Vicepresidencias. Las líneas de trabajo de esta coalición están centradas en "generar cultura de ciberseguridad, ofrecer apoyo a la Industria e I+D+i" (Foro Nacional de Ciberseguridad, 2020), medidas que se recogen en el informe *Estrategia Nacional de Ciberseguridad 2019* (Presidencia del Gobierno, 2019).

Aunque está por demostrar su eficacia contra la desinformación, debido a que se encuentran en fase inicial, se confía plenamente en la labor realizada por los observatorios públicos de medios de comunicación. La Comisión Europea, a través del European Digital Media Observatory, ha impulsado el proyecto *Iberian Digital Media Research and Fact-Checking Hub* (Iberifier). El objetivo de esta iniciativa, liderada por el profesor e investigador Ramón Salaverría, es fortalecer la resiliencia social mediante la participación de 23 instituciones españolas y portuguesas (universidades, verificadores y agencias de noticias y centros de investigación multidisciplinar) y 70 investigadores de medios digitales de máximo nivel**.** Iberifier se presenta, por tanto, como una solución holística para combatir los desafíos que en torno a la desinformación se enfrenta la sociedad hispano-portuguesa (Iberifier, 2021).

El programa de innovación e investigación Horizonte 2020 ha movilizado recursos para abordar la veracidad de la información que se presenta en las redes sociales y en los medios de comunicación. En el marco de este programa se han desarrollado proyectos con participación española. Por ejemplo, el proyecto *Co-inform*, que desarrolla herramientas destinadas a fomentar el

Foto 9: Un visitante pasa ante un holograma en el Mobile World Congress de Barcelona (MWC), en una edición, la de 2022, en la que el 5G fue uno de los grandes protagonistas. EFE/Quique García



pensamiento crítico y la alfabetización digital para una sociedad mejor informada (Young, s.f.). El proyecto *TRESCA*, que promueve el aumento de la confianza en la ciencia y la innovación gracias a prácticas de comunicación innovadoras de investigadores científicos, periodistas y responsables políticos (Fattori, 2020). Además, el Consejo Europeo de Innovación también ha impulsado actuaciones de entidades verificadoras españolas. Por ejemplo, *Newtral* ha conseguido desarrollar un sistema semiautomático de detección de noticias falsas en tiempo real.

Desde la Universidad española surge la cátedra Jean Monnet sobre "Unión Europea, Desinformación y Fake News". Esta iniciativa, vinculada a la Universidad Carlos III de Madrid, aborda la desinformación y los bulos desde dos enfoques: el periodismo y la ciencia. Ambas disciplinas se complementan para actuar "como herramientas fundamentales para luchar contra las noticias maliciosas" (Universidad Carlos III de Madrid [UC3M], s.f.). A los proyectos citados, se han sumado numerosas iniciativas académicas que han contribuido a aumentar el ecosistema de conocimiento sobre desorden informativo y los bulos.

La crisis sanitaria ha generado, según las estadísticas extraídas de las principales bases de datos académicas, una ingente cantidad de trabajos de investigación. Asimismo, gran parte de los estudios en los últimos años surgen de colaboraciones interdisciplinares, reafirmando que la lucha contra la desinformación debe partir de un enfoque holístico. Estos trabajos, algunos realizados apresuradamente, han permitido conocer mejor el modo de operar y las manifestaciones del fenómeno desinformativo en entornos digitales. La Academia, en este caso, ha resultado fundamental para resolver el laberinto semántico que circunda a la desinformación (Salaverría et al., 2020); ha arrojado luz sobre las correlaciones de la creencia de las noticias falsas en España (Wiesehomeir y Flynn, 2020) y ha profundizado en las metodologías innovadoras de los verificadores españoles de datos (Rodríguez-Martínez et al., 2021), entre otros muchos temas.

A día de hoy, el número de estudios publicados sobre el binomio desinformación y educación mediática no es muy extenso. Sin embargo, las aportaciones realizadas por autores de reconocido prestigio resultan significativas (MacDougall et al., 2019). Ya no resulta novedosa la propuesta de una educación cívica que incluya la alfabetización en medios de comunicación como una solución sostenible a la problemática del fenómeno desinformativo. La alfabetización mediática no hace magia, pero proporciona recursos y habilidades que permiten juzgar la credibilidad de la información y auditar las fuentes afines al ideario de cada individuo.

A día de hoy, el número de estudios publicados sobre el binomio desinformación y educación mediática no es muy extenso. La alfabetización mediática proporciona recursos y habilidades que permiten juzgar la credibilidad de la información y auditar las fuentes.

La Alfabetización Mediática e Informacional (AMI) en la Educación Secundaria Obligatoria

Según el Instituto Nacional de Estadística, en 2020, 37,3 millones de personas de 10 y más años ya han accedido a Internet en alguna ocasión. Entre los/as niños/as de 10 a 15 años se ha producido un incremento interanual de internautas del 3,1%, alcanzando los 2,8 millones (Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información [ONTSI], 2020), una tendencia que continúa en aumento. El último informe de la Sociedad de la Información, elaborado por Fundación Telefónica, indica que prácticamente todos los jóvenes de entre 16 y 24 años son usuarios de Internet (99,1 %) y el 93,6 % es, además, usuario frecuente (Rodríguez Canfranc et al., 2020, p. 38). Los datos confirman una realidad evidente: los adolescentes están continuamente conectados y más expuestos que nunca al contenido mediático que se genera en las diversas plataformas en las que se mueven (Whatsapp, TikTok, Twitch o similares).

Foto 10: Estudiantes de educación secundaria de un instituto de Toledo. EFE/Ismael Herrero

Según el Instituto Nacional de Estadística (2020), el 69,5% de la población de 10 a 15 años dispone de teléfono móvil frente al 66,0% de 2019, teléfonos móviles que están continuamente conectados a la red. A pesar de que la digitalización española es una realidad, los niveles de competencias digitales básicas de la población española son inferiores a la media de otros países: "Poco más de la mitad de las personas entre 16 y 74 años posee capacidades digitales básicas" (Rodríguez Canfranc et al., 2020, p. 38). Lo que nos lleva a plantearnos si más allá de la adquisición de competencias digitales somos capaces, como sociedad, de ir un paso adelante que nos permita conseguir una alfabetización no solo tecnológica sino también crítica y comprensiva, donde la escuela juega un papel fundamental.

A pesar de que la digitalización española es una realidad, los niveles de competencias digitales básicas de la población española son inferiores a la media de otros países.

> "La escuela debe acometer y desarrollar el modelo de alfabetización múltiple destinado a que el estudiante adquiera las competencias instrumentales, cognitivas, actitudinales y axiológicas para un uso inteligente y crítico de la información" (Area Moreira et al., 2008, p. 87).

El sistema educativo español ha experimentado 8 reformas o leyes educativas a lo largo de su historia democrática, contando con la última Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOMLOE, 2020) aprobada el pasado mes de noviembre en el Congreso de los Diputados. Sin embargo, no es hasta la Ley Orgánica 10/2002, de 23 de diciembre, de Calidad de la Educación, (LOCE, 2002) cuando se empieza a hacer referencia, de forma explícita, a los cambios y transformaciones "tecnológicas" y a la conveniente necesidad de incorporar en las distintas etapas educativas contenidos relacionados con las Tecnologías de la Información y las Comunicaciones (TICs), tal y como se expone en el preámbulo de la ley:

> "Exige también que los alumnos puedan adquirir destrezas que, como la capacidad de comunicarse —también en otras lenguas—, la de trabajar en equipo, la de identificar y resolver problemas, o la de aprovechar las nuevas tecnologías para todo ello, resultan hoy irrenunciables" (LOCE, 2002).

Estas competencias relacionadas con las TICs aparecen articuladas como uno de los objetivos de la Educación Secundaria Obligatoria, en el apartado *c* del artículo 22: "Desarrollar destrezas básicas en la utilización de las fuen-

tes de información para, con sentido crítico, adquirir nuevos conocimientos", así como en el apartado *h*: "Adquirir una preparación básica en el campo de las tecnologías fundamentalmente, mediante la adquisición de las destrezas relacionadas con las tecnologías de la información y de las comunicaciones, a fin de usarlas, en el proceso de aprendizaje, para encontrar, analizar, intercambiar y presentar la información y el conocimiento adquiridos".

En esta misma ley se hace referencia a la autonomía de los centros para impulsar o desarrollar proyectos relacionados con el ámbito de la información:

> "Los centros docentes, en virtud de su autonomía pedagógica y de organización establecidas en la presente Ley, y de acuerdo con el procedimiento que establezcan las Administraciones educativas, podrán ofrecer proyectos educativos que refuercen y amplíen determinados aspectos del currículo referidos a los ámbitos lingüístico, humanístico, científico, tecnológico, artístico, deportivo y de las tecnologías de la información y de las comunicaciones" (Artículo 66.1).

Estas aportaciones de la LOCE (2002) con respecto a la educación mediática y las Tecnologías de la Información y Comunicación se siguen manteniendo en las leyes posteriores, otorgando cada vez más importancia al relevante papel que tienen hoy en día las competencias digitales no solo para los estudiantes sino también para el profesorado. Así, la Ley Orgánica 2/2006, de 3 de mayo, de Educación, 2006 (LOE, 2006) sobre la *Formación Permanente del Profesorado en Centros Públicos* indica que:

> "Las Administraciones educativas promoverán la utilización de las tecnologías de la información y la comunicación y la formación tanto en digitalización como en lenguas extranjeras de todo el profesorado, independientemente de su especialidad, estableciendo programas específicos de formación en estos ámbitos" (Artículo 103).

Sin embargo, no es hasta la actual ley de educación donde se comienza a hablar de términos como "sociedad digital", "consumo responsable y uso crítico" de los medios de comunicación y en el que se señala que las administraciones educativas deben incluir estos aspectos en el desarrollo curricular de lo que se ha venido conociendo como competencia digital.

Se trata, por tanto, de ir un paso más allá de la simple instrumentalización de la tecnología y basarse no solo en el "hacer", sino también en el "saber hacer".

La exministra de Educación Isabel Celaá[3] destacaba en el mes de junio de 2021, hablando sobre el nuevo currículo, la importancia de formar a ciudadanos "éticos que sepan diferenciar la información de la opinión en el mundo que vivimos".

En cuanto a la normativa básica nacional sobre el currículum y los contenidos que se imparten en las distintas etapas educativas, en especial en Secundaria y Bachillerato, las competencias relacionadas con el uso y comprensión de las tecnologías de la información y Comunicación se articulan como elementos transversales del propio currículum. Lo que permite la autonomía a los propios centros para incluir o articular asignaturas optativas más específicas.

En la Orden ECD/65/2015, de 21 de enero, por la que se describen las relaciones entre las competencias, los contenidos y los criterios de evaluación de la educación primaria, la educación secundaria obligatoria y el bachillerato (BOE, 2015) se habla de cómo gestionar la información y ponerla a disposición de los usuarios "sabiendo elegir aquellos que responden mejor a las propias necesidades de información."

Por lo tanto, nos encontramos ante destrezas vinculadas con el tratamiento de la información, la lectura multimodal y la producción de textos electrónicos en diferentes formatos. Unas competencias que van más allá de "lo digital" y que ponen el acento en "el uso creativo, crítico y seguro" de las tecnologías de la información y la comunicación.

Desde el proyecto *Alfabetización mediática en los centros de secundaria. ¿Cómo se enseña a los adolescentes a consumir información?*[4], se considera necesario revisar los contenidos curriculares que afectan a la etapa de secundaria, puesto que es el momento donde más expuestos están a la información tanto por accesibilidad como por dispositivos (Herrero Curiel y la-Rosa Barrolleta, 2021) y, sin embargo, la maduración emocional de este segmento de la población nos lleva a pensar que no tienen recursos suficientes para asimilar de forma constructiva tanta información.

En la investigación anteriormente mencionada, en la que han participado 70 centros de educación secundaria de naturaleza pública y repartidos por

[3] Declaraciones realizadas durante la inauguración del foro de estudiantes y familia Nuevo Currículo para nuevos desafíos en https://curriculo.educacion.es/

[4] Realizado con la Beca Leonardo a Investigadores y Creadores Culturales 2020 de la Fundación BBVA más información sobre la investigación en curso: https://www.uc3m.es/investigacion/alfamedeso

toda España, se ha detectado que la mayoría de los centros contemplan la alfabetización mediática como un contenido transversal que depende, exclusivamente, de la voluntad docente. Una voluntad limitada por el tiempo y el excesivo contenido curricular que el profesorado está obligado a dar en secundaria, por tanto, la motivación para llevar al aula esta alfabetización es baja.

Por otro lado, existen diferencias significativas entre centros educativos dependiendo del nivel socioeconómico y cultural de las familias de procedencia de los estudiantes lo que contribuye a generar una brecha importante entre estudiantes de la misma etapa educativa. Por ello, la educación mediática debe estar integrada en la educación formal de una manera homogénea en todos los centros y complementada por espacios no formales, de manera que las familias también puedan tener acceso a una educación en medios. Se trata de una competencia holística que va más allá del aula.

La educación mediática debe estar integrada en la educación formal de una manera homogénea en todos los centros.

La importancia de la alfabetización mediática en el aula tendría como fin que los estudiantes desarrollen, entre otras cosas, “un metalenguaje, una forma de discurso crítico, con el que estarán en condiciones de describir y analizar los acontecimientos en curso” (Buckingham, 2005, p. 267). En definitiva, contribuir a que los estudiantes se conviertan en ciudadanos críticos dentro de un mundo globalizado, complejo y en continua transformación tecnológica.

PROPUESTAS DE DEFINICIÓN

Ámbitos de desinformación a tratar desde la alfabetización mediática

Exceso de información

Prensa, radio, televisión, redes sociales, plataformas digitales, blogs, correos electrónicos, publicidad, cartelería, mensajería instantánea, servicios de entretenimiento en línea, etc. nos bombardean día a día sin que seamos conscientes del volumen de información que impacta en cada uno de nosotros a lo largo del año. La mayoría de estos estímulos pertenecen a nuestra cotidianidad sin que seamos conscientes de la avalancha de información a la que estamos expuestos. La falta de tiempo material para poder realizar una reflexión crítica sobre el contenido y el significado de todo a lo que estamos expuestos conlleva una incapacidad cognitiva definida como "exceso de información".

Aun así, el cerebro realiza una selección de la información de manera inconsciente, es lo más cercano a lo que podemos llamar "zapping mental". Pero no es suficiente. Vivimos en una paradoja continua donde tenemos una gran facilidad para acceder a la información y, a su vez, resulta imposible realizar lecturas analíticas y sosegadas de todos esos mensajes. Según un informe de la Organización Mundial de la Salud (2 de febrero de 2020) existe "Una sobreabundancia de información –alguna exacta y otra no– que hace difícil que la gente encuentre fuentes dignas de crédito y fiables". Esto conlleva una dificultad a la hora de distinguir entre informaciones fiables y falsas, una situación que produce una sensación de saturación e, incluso, de más desinformación que información. El acrónimo infodemia define esta realidad en la fusión de las voces información y epidemia y que se emplea "para referirse a la sobreabundancia de información (alguna rigurosa y otra falsa) sobre un tema" (Fundéu, s.f.).

Vivimos en una paradoja continua donde tenemos una gran facilidad para acceder a la información y, a su vez, resulta imposible realizar lecturas analíticas y sosegadas.

Se puede concluir que nos hemos acostumbrado a recibir los mensajes fragmentados, reducidos, sintetizados. Para competir en este bullicioso conglomerado, los mensajes se construyen de la forma más atractiva posible y para el consumo rápido. En cierta forma, implica el regreso a las teorías clásicas de los medios de comunicación: "la bala mágica" y la "aguja hipodérmica", dos metáforas que ilustraban la rapidez, indefensión y precisión de los mensajes de los medios de comunicación. Las tradicionales seis W's del periodismo: qué (*What*) ha sucedido; quiénes (*Who*) son sus protagonistas; dónde (*Where*) ha sucedido; cuándo (*When*) ha sucedido; y por qué ha sucedido (*Why*); junto con otra más: cómo (*How*) ha sucedido el hecho; cada vez se presentan con menos frecuencia en las informaciones. La información se registra, principalmente, a través de titulares que emplean el *clickbait* (el engaño) para animarnos a pinchar en el enlace. Apostando por mucha cantidad de información (muchos clicks), pero de poca profundidad.

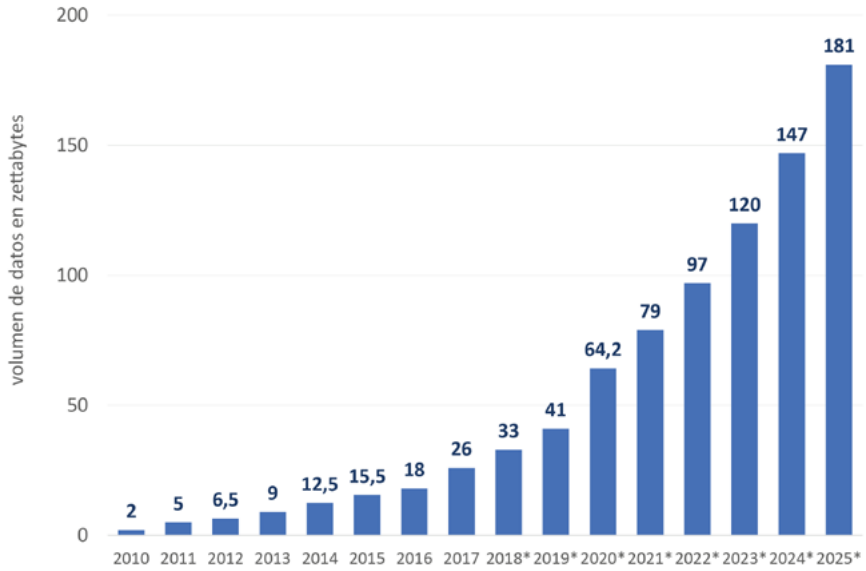


Gráfico 4: Volumen de datos/información creada, capturada, copiada y consumida en todo el mundo de 2010 a 2025 (en zettabytes). Fuente: Statista, 2021[5]

[5] Las cifras de 2021 a 2025 fueron calculadas por Statista en base a la cifra de pronóstico de 2020 y la tasa de crecimiento anual compuesta (CAGR) de cinco años del 23 por ciento proporcionada por la fuente. Las cifras anteriores a 2020 se basan en el pronóstico de IDC de finales de 2018. (Fuente: Statista, 2021)

Además, nos exponemos no solo a los medios, como intermediadores de la información. Ahora los protagonistas de ésta también nos informan de sus actos y podemos interactuar directamente con ellos. Las plataformas digitales como las redes sociales permiten que cualquier persona se convierta en generador de contenidos y, por tanto, pueda propagar noticias (tanto verdaderas como falsas o, al menos, no contrastadas). El gráfico 1 refleja esta realidad. Según el Statista (2021), el volumen de datos/información creada, capturada, copiada y consumida en todo el mundo en 2021 supera los 79 zettabytes. Sin ir más lejos, en 2020 las personas crearon 1,7 MB de datos por segundo, los usuarios enviaron alrededor de 500.000 tuits/día y se remitieron 306,4 mil millones de correos electrónicos por día. Para 2025, casi 200 zettabytes de datos estarán almacenados en la nube en todo el mundo.

Ya en 1970, Alvin Toffler acuñó el término de exceso de información (*information overload*) en su libro *Future Shock,* donde ya vaticinaba que el auge de la tecnología llenaría nuestra vida diaria de datos e información. "Nuestro poder tecnológico aumenta, pero los efectos colaterales y los peligros potenciales también se intensifican" (Toffler, 1970). Esto incrementa la necesidad que tiene cada persona de reconocer la *buena* información entre todo el "ruido" que hay alrededor, interferencias que perturban al proceso de comunicación y que debemos de ser capaces de identificar para lograr una información verdadera y verificada y no caer en los rumores, bulos o falsedades.

Este exceso o saturación de información genera también desconfianza sobre lo que se lee, se escucha o se ve. De tal forma que se complica exponencialmente las relaciones entre los medios y el público. Ya no se confía como antes en los medios puesto que no es tan seguro que el medio haya realizado el filtrado que se le presupone a la información verídica. Los medios buscan abarcar mucho terreno informativo más que profundizar en el mismo. Este hecho implica la desconfianza del público ante la falta de calidad y de rigurosidad. Por otra parte, el público también es partícipe al generar o compartir información irrelevante sin contrastar, por el mero hecho de intervenir en el tráfico comunicativo.

En definitiva, cada día nos enfrentamos con un número mayor de impactos informativos. Y a mayor cantidad de contenidos, mayor es nuestra incapacidad para digerir tanta información.

A mayor cantidad de contenidos, mayor es nuestra incapacidad para digerir tanta información.

El exceso de información desde el Derecho

Para ilustrar el propósito del exceso de información provocado de manera intencionada podemos recordar la expresión “si no puedes con el enemigo, confúndelo”. La saturación de contenidos no siempre busca manipular comportamientos para dirigirlos en una determinada dirección, busca más bien perturbarlos hasta degradar la capacidad crítica del individuo y hacerle incapaz de tomar decisiones o hacer que las adopte arbitrariamente, conforme a criterios poco ajustados a la realidad que le rodea.

¿Cómo puede la ley acometer este fenómeno en el mundo digital? ¿Cómo “desenredar” la desinformación de la información? Por una parte, debe estar claro que no se pretende ganar una guerra, sino que la intervención del Derecho pretende garantizar la paz y que por eso las medidas adoptadas tienen que respetar límites, especialmente si afectan a los derechos fundamentales. Por otra parte, las autoridades deberán intervenir solo en función de sus competencias constitucional y legalmente atribuidas, así como con la proporcionalidad que requiera el tipo de caos/daño generado y el tipo de contenido concreto que se pretendan “desenquistar”. Así, se podrán denunciar delitos, ilícitos civiles o administrativos y seguir los trámites procesales oportunos. Ya existen previsiones legales para esto, pero lo que no hay es “eficiencia” (en este sentido ya se abordan en el Capítulo 2 se ocupa de aportar aspectos vinculados con la regulación).

Necesitamos protocolos de actuación adaptados a lo digital. Que individuos, empresas y administraciones sepan y puedan desenmarañar la información que les afecta, tomar decisiones de manera transparente y rápida para visibilizar lo que corresponde a su propia imagen y la realidad de su actuar.

Faltan recursos organizativos y materiales que lo permitan, que les ayuden en esta tarea. No se sabe el origen del caos informativo porque normalmente proviene de diferentes vectores “de ataque”. Pero se sabe a quién afecta. Demos por tanto visibilidad a la información que estos afectados promueven, a la información veraz, información científica, información institucional, etc., “iluminándolo” en el escaparate de las principales plataformas y medios. Esta información veraz sí se puede controlar, se sabe de quién proviene, al que afecta, su realidad, su actuar, su trabajo, sus funciones y, por tanto, se les podría identificar perfectamente si en vez de tratar de evitar dispersiones promovieran más el caos con la respuesta.

Un problema diferente lo tenemos cuando el caos se origina con informaciones institucionales no contrastadas, no científicas, descoordinadas, etc., pues la confusión anima a buscar respuestas, y anima a responder, a cualquiera, sumándose más informaciones de dudosa procedencia e intención.

Actualmente, con un sentido práctico mal entendido, se está dejando en manos de la "infantería", de los proveedores de servicios, delimitar la verdad de lo falso, desenmarañar el ruido y dejar la información "limpia", bajo criterios legales de responsabilidad proactiva, directa y objetiva. Mientras que lo realmente operativo sería que tuvieran protocolos de comunicación y posterior actuación, estandarizados y ajustados a Derecho, en la colaboración público privada.

Sea como fuere, de nuevo, la educación es la base para generar pensamiento crítico y comprender la coexistencia de informadores y desinformadores. Pero sin la confianza en las instituciones nunca podremos ordenar el impacto del exceso de información. Y el Derecho es la herramienta para determinar: la responsabilidad de estas (responsabilidad objetiva), la forma de emitir la información oficial, la colaboración con las plataformas para que sea correctamente comunicada y visibilizada; la libertad de información para que, en su caso, pueda ser rebatida (verazmente), etc.

La educación es la base para generar pensamiento crítico y comprender la coexistencia de informadores y desinformadores.

La desinformación y los bulos

El universo semántico de la desinformación es increíblemente amplio. El castellano reconoce, de forma somera, un amplio número de palabras que dan cuenta de ese propósito de confusión faltando a la verdad: infundio, bulo, insidia, calumnia, manipulación, desinformación, patraña, posverdad, pajarota, falacia, paparrucha, andrómina, mentira, chisme, filfa o trola (Lascuráin, 2020). El término bulo destaca, en su definición de la RAE, por su objetivo pragmático ("noticias falsas propagadas con algún fin"). Por ello, en el bulo se entremezcla el interés dañino por divulgar algo oculto que se considera negativo con la falsedad sobre aquello que se está divulgando.

Los límites de este concepto son difusos. Diversos autores que han realizado propuestas clasificatorias o aclaratorias en cuanto a los términos relacionados con la desinformación, subrayando que es mejor evitar la expresión "noticias falsas" y sustituirla por otras como noticias falseadas o bulos (Wardle, C., 2017; Pérez Tornero et al., 2018; Salaverría et al., 2020). Puede tomarse como marco consensuado la definición general que propone la Comisión Europea sobre desinformación para comprender el contenido al que se trata de combatir: "Información falsa, inexacta o engañosa diseñada, presentada y promovida para causar daño público intencionalmente o con fines de lucro. El riesgo de daño incluye amenazas a los procesos y valores políticos democráticos, y pueden dirigirse específicamente a una variedad de sectores como la salud, la ciencia, la educación, las finanzas y más" (Comisión Europea, 2018). De idéntica manera, hay autores que prefieren la denominación "fact-checking" y otros la de "verificación". Fundéu recomienda este segundo término (Fundéu, s.f.).

La lucha contra los bulos digitales no es nueva y en España se ejerce bajo la etiqueta #stopbulos desde 2012 por parte de la organización de voluntarios digitales VOSTSpain. La gravedad de los efectos de los bulos sobre la ciudadanía y su influencia en los procesos de desinformación han promovido la aparición de "plataformas de verificación" (*fact-checking*). La mayor parte de ellas se encuentran coordinadas por la International Fact-Checking Network (fundada en 2015 por el Poynter Institute for Media Studies) que, en la actualidad, incluye a 92 plataformas de verificación de todo el mundo. Su objetivo es desmentir los bulos, pero su proliferación en determinados periodos o frente a determinados eventos (en el marco del exceso de información definido en el epígrafe anterior) implica una saturación de estas plataformas en el proceso de identificación y/o divulgación de estos bulos. Una circunstancia que ha reflejado el informe Top Strategic Predictions for 2018 and Beyond, que

alerta de que el público occidental consumirá más noticias falsas en 2022 que noticias verdaderas debido a la imposibilidad de establecer fórmulas efectivas para frenar su propagación (Gartner, 2017). En el Observatorio Europeo contra la Desinformación (EDMO), creado en 2020, se acoge a las plataformas de verificación europeas con un concepto amplio que va del *fact-checking* político a la verificación avanzada o investigación con fuentes abiertas (OSINT). La Academia también tiene cabida en este importante polo europeo contra los bulos.

Una investigación de la Universidad de Navarra y el Centro Nacional de Supercomputación desarrolla un "diagrama de gravedad de los bulos" y explica los criterios de discriminación y atención de estas plataformas (Gráfico 2). En esa imagen se puede apreciar dos coordenadas que marcan la gravedad de los bulos (falsedad y voluntariedad), a partir de una muestra que revisaron *Maldita.es*, *Newtral* y *EFE Verifica* durante la pandemia sanitaria de la COVID-19.

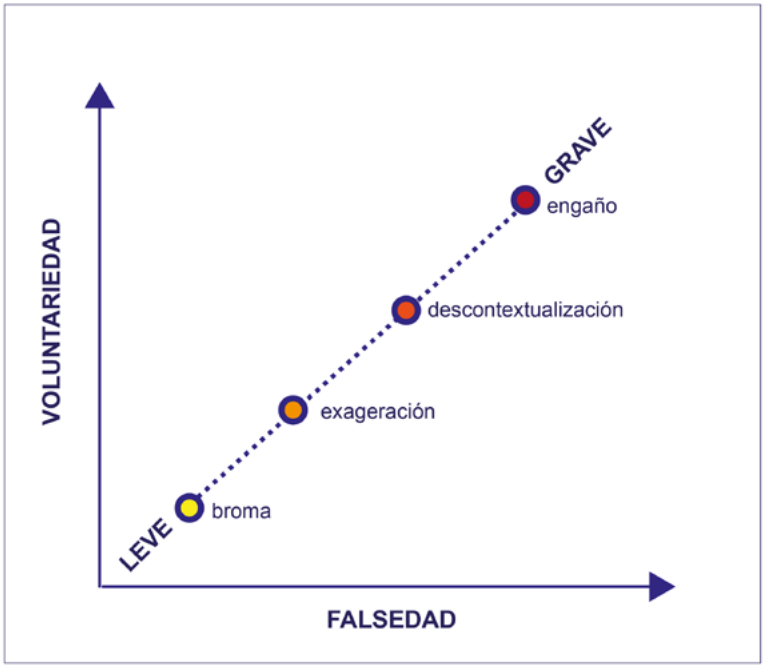


Gráfico 5: Diagrama de gravedad de los bulos. Fuente: Salaverría et al. 2020

Esta gradación implica que aquellos bulos que puedan tener un mayor efecto desestabilizador deben ser desmentidos con la mayor contundencia y brevedad posibles. Sin embargo, esa circunstancia implica que un amplio número de bulos "de menor categoría" (bromas o exageraciones principalmente) pueden pasar inadvertidos por estas plataformas y, sin embargo, tener una influencia significativa sobre la opinión pública y la ciudadanía.

Aquellos bulos que puedan tener un mayor efecto desestabilizador deben ser desmentidos con la mayor contundencia y brevedad posibles.

Esta incapacidad para cubrir todo el espectro de los bulos por parte de organismos e instituciones impulsa la necesidad de dotar de herramientas e instrumentos a la ciudadanía. Una de las formas más habituales de definir este proceso es el de la "alfabetización mediática" que persigue formar a usuarios críticos con la información que reciben a través de los múltiples canales que la tecnología ofrece en estos tiempos.

Los diferentes apartados de este capítulo profundizan en ese proceso desde diferentes puntos de vista (entre otras, identificación de los colectivos más vulnerables y los objetivos de las diferentes estrategias de alfabetización). Para ello, se parte de una serie de recomendaciones para determinar cuándo se está frente a un bulo o alguna estrategia de desinformación:

- Si una "primicia informativa" genera sentimientos o emociones intensas -especialmente de sorpresa, desagrado, enfado, etc.- convendría verificarla.
- Un exceso de noticias que reafirman nuestra visión del mundo o nuestra opinión, requieren ser contrastadas para asegurar que no hemos creado, a nuestro alrededor, una cámara de eco (*echo chamber*).
- Cualquier artículo o noticia que aparece sin sus datos básicos (fecha, fuente o autor, por ejemplo) presenta indicios de haber sido "fabricado".
- A partir de lo anterior, conviene tener en cuenta que la desinformación y los bulos tienen muchas formas: memes, fotografías, vídeos, capturas de pantalla o falsos sitios webs de noticias. Es necesario desarrollar una capacidad crítica para reconocer las características de cada uno de estos medios.
- El alcance de fiabilidad de una fuente. La fiabilidad que podemos darle a un reputado experto en una materia debe recalibrarse cuando

nos esté contando algo que no sea de su campo de conocimiento. Como se ha señalado, en ocasiones, los bulos se difunden a través de alguna de nuestras fuentes de confianza que nos lo trasladan de forma ingenua, sin haberse revisado su veracidad.

Colectivos a los que dirigir las acciones de alfabetización

Estudiantes de educación Primaria, Secundaria, Bachillerato y Universidad

La alfabetización mediática e informacional ha tenido experiencias ya antiguas en el programa Prensa de Escuela que desarrolló el MEC en los años ochenta y noventa del pasado siglo. Al mismo tiempo, otros programas ministeriales como el Mercurio y el Atenea también realizaron acciones institucionales que tuvieron un afán inicial de formación del profesorado con un carácter más tecnológico que de formación de la actitud crítica de los estudiantes. En diferentes comunidades también se produjeron programas de carácter autonómico como fue en Andalucía (Zahara XXI), en Asturias (EDUCASTUR) y en Cataluña los emprendidos por el Consell de l'Audiovisual de Catalunya (CAC) y anteriormente por el Departamento de Enseñanza de la Generalitat de Cataluña. Lo cierto es que en estas décadas ha habido muchas cosas que han cambiado en el nuevo contexto digital, con el auge de Internet y la ampliación de las redes sociales. La formación de los estudiantes de los diferentes niveles educativos implica también la formación del profesorado.

La UNED lanzó un programa pionero de alfabetización mediática en el año 1987, denominado Curso de Iniciación a la lectura de la Imagen y al conocimiento de los MAVs (Aparici et al., 1987) que se mantuvo a lo largo de décadas y que -solo en su primer año- formó a más de 1.000 profesionales de la educación de diferentes niveles educativos. En enero de 2021, la asociación Iberoamericana ALFAMED, presentó el Currículum ALFAMED de formación de profesores en Educación mediática (Aguaded et al., 2021) y en octubre del mismo año se presentó la versión brasileña, en lengua portuguesa.

Las investigaciones realizadas en los últimos años sobre la competencia mediática por grupos de investigación coordinados de las universidades Pompeu Fabra de Barcelona, Universidad de Huelva y Universidad de Valladolid, muestran que el nivel de competencia mediática de profesores y estudiantes de los diferentes niveles educativos es muy deficiente (Ferrés et al., 2012). Estos estudios aportan datos muy preocupantes que prueban el analfabetismo funcional de los jóvenes en muchas de las competencias

mediáticas e informacionales definidas y también la necesidad de actualización de los propios profesionales de la comunicación (Buitrago et al., 2015). Los principales argumentos a favor que se encontraron eran los siguientes:

- Aunque están muy familiarizados con el uso de internet porque son nativos digitales tienen dificultades para distinguir la información fiable de la errónea y la desinformación de la opinión.
- La alfabetización mediática e informacional va a contribuir a una formación útil para que los jóvenes tengan una mayor comprensión de los contextos sociopolíticos en los que viven y sean más activos y participativos en los procesos de enseñanza-aprendizaje.
- Son los votantes del futuro y necesitan herramientas sólidas para poder ejercer su derecho al voto.
- La mayoría no tiene ninguna formación para desarrollar el pensamiento crítico que les permita valorar la calidad de la programación de los diferentes medios y la información en medios de comunicación tradicionales como la prensa escrita, la radio, la televisión e internet.
- La Universidad Complutense de Madrid impartió en 2012 los primeros seminarios específicos sobre verificación digital contra la desinformación en redes para estudiantes de periodismo. Y en el año 2017-18, la Universidad Francisco de Vitoria (UFV) impartió esta materia como asignatura cuatrimestral por primera vez en el panorama universitario español.

En España, más de la mitad de los españoles son vulnerables ante la desinformación, especialmente los jóvenes y los mayores (Ballesteros Guerra y Picazo Sánchez, 2018). En estos estudios se destaca que solo el 22,5% de adolescentes españoles de 14 a 16 años afirma haber recibido formación sobre el desarrollo de pensamiento crítico para valorar la información en Internet. Otros estudios internacionales confirman la necesidad de dar una educación crítica a los más jóvenes que mejore su capacidad para informarse en internet. En EE. UU., más de la mitad de los estadounidenses admiten compartir noticias inventadas en línea. La mayoría de ellos no sabían que era falso cuando lo compartieron. Aunque los adolescentes con conocimientos digitales han crecido en internet, una investigación del *Stanford History Education Group* muestra que la gran mayoría tiene problemas para navegar por la información digital y distinguir la información de calidad y fiable de bulos que se publican en redes sociales o contenido patrocinado en sitios de noticias, por ejemplo (Breakstone et al., 2019).

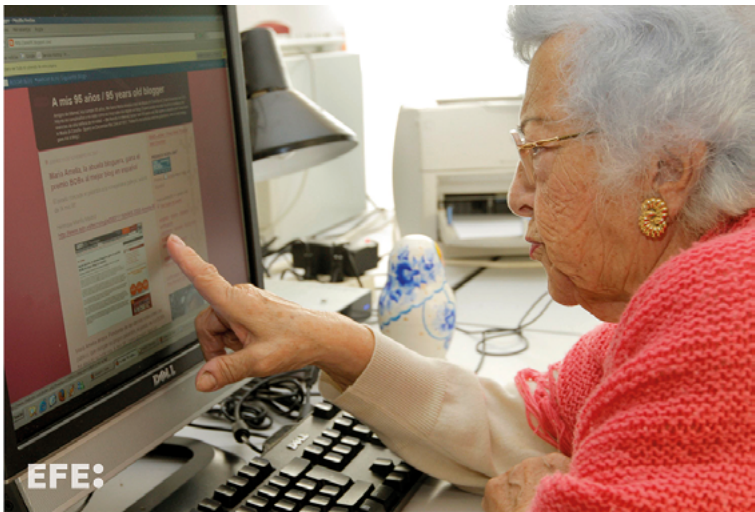
Tercera edad

La pandemia ha puesto de manifiesto el drama de la falta de atención a nuestros mayores. Ellos han sido el sector de población más afectado por la tragedia de la pandemia. Como sociedad debemos saber que el nivel de motivación de las personas mayores de 60 años es muy elevado y a esto se añaden los datos que nos dicen que, a pesar de la tragedia vivida por la COVID-19, la esperanza de vida de los mayores va a volver a ser muy elevada y esto exige extender esos procesos de alfabetización mediática e informacional a este sector poblacional, con el objetivo de evitar una desconexión que tiene incidencia directa en la calidad de vida de nuestros mayores e implicaciones directas en el ámbito de la salud. Podemos señalar los siguientes argumentos a favor:

- Los mayores de 50 son quienes más noticias falsas comparten (hasta 7 veces más (Herrero-Diz et al., 2020)). Lo confirman varios estudios internacionales (Guess et al., 2019 y 2020).
- Son los mayores consumidores de Radio y Televisión con consumos que superan de media las 7 horas diarias de televisión.
- Las deficiencias cognitivas de los mayores les hacen más vulnerables ante la desinformación. Les cuesta más identificar "fake news", porque ello exige un esfuerzo cognitivo, y tienen más facilidad para olvidar el origen de una información (esto hace que den por cierta una información que ven en repetidas ocasiones (Skurnik et al., 2005)). También presentan más dificultades para distinguir entre opinión e información (Gottfried et al., 2018).

Las deficiencias cognitivas de los mayores les hacen más vulnerables ante la desinformación.

Foto 11: Una usuaria de internet de 95 años. EFE/Lavandeira jr.



- Además, las personas mayores tienden a confiar más en los demás (Poulin y Haase, 2015).
- A menudo tienen escasas destrezas digitales y, al mismo tiempo, un porcentaje significativo tiene altas expectativas en el uso de las TICS. En EEUU, los adultos de más de 50 años son responsables (Ragiboglu, 2020) del 80 % de la difusión de noticias falsas en Twitter y los mayores de 65 las ven en Facebook siete veces más que los usuarios de menos edad. En definitiva, que los mayores son quienes más comparten, y de ese modo difunden, noticias falsas (Brashier y Schacter, 2020).

Colectivos especialmente vulnerables

Personas con capacidades diferentes que hallan una mejor integración valiéndose de los medios de información y comunicación. Son especialmente receptivos a un trabajo creativo y dinamizador. Su contacto con los medios es para ellos motivador y les ayuda a explotar esas capacidades especiales que los diferencian y además son un incentivo para su integración. En este apartado hay que hacer una alusión especial a la población reclusa a la que se cita en el artículo 25.2 de la Constitución española. La reeducación y reinserción de los penados es un objetivo constitucional. Las condiciones actuales de las cárceles impiden que hasta ahora esa educación en competencia mediática e informacional se pueda realizar, lo que producirá una nueva forma de analfabetismo funcional y mayor riesgo de aislamiento e imposibilidad de reinserción en el actual contexto digital y, por lo tanto, mayor riesgo de reincidencia, lo que implica un coste mucho más elevado que el que supondría atender a esa formación integral de la población reclusa.

Las condiciones actuales de las cárceles impiden que hasta ahora esa educación en competencia mediática e informacional se pueda realizar.

Entre los argumentos a favor se encuentran:

- Están especialmente motivados ante estímulos que faciliten la comunicación.
- Tienen un acceso más limitado a la información de calidad, bien por falta de recursos económicos, como de tiempo o formación.
- En el caso de la población reclusa, suponen una inversión que implica retornos económicos mucho más elevados, por lo que representa evitar el dolor que implica cumplir de forma profunda con el mandato constitucional y evitar el dolor que representa el aumento de una acción criminal que pueda ser cada vez más elevada y nociva para el conjunto de la sociedad.

Formadores

El profesorado de los diferentes niveles educativos debe conocer metodologías de enseñanza que permitan aprovechar las inmensas posibilidades de los medios de comunicación tradicionales, de las TICs y de las redes sociales, evitando la demonización de las mismas y tomando una actitud proactiva para que los propios adolescentes sientan que desde la educación se les da participación en su formación. Por ello, se considera que un argumento a favor es la necesidad de conocer las herramientas disponibles para hacer frente a la desinformación y las tendencias actuales con las que se desinforma.

Periodistas y medios de comunicación

Las investigaciones más recientes muestran la opinión favorable de los profesionales de la información y de la comunicación a la inclusión de la educación en competencia mediática en su propia actualización profesional. (Buitrago et al., 2015) Aceptan las carencias generales a la hora de incorporarse al actual contexto digital. Los argumentos a favor que se han localizado subrayan que:

Lo primero es compartir un consenso que ya es asumido por muchos profesionales del periodismo y que lleva a la convicción de que los medios, Internet y las redes sociales tienen capacidad para educar y deseducar y que es importante convencer a los jóvenes de la importancia del periodismo de calidad. Las asociaciones de Prensa y la propia Federación de Asociaciones de Periodistas de España (FAPE) o los Colegios Profesionales, agrupados en la Red de Colegios, así como otras organizaciones profesionales, tienen un papel crucial. La FAPE promovió, en 2013, el primer curso online de Periodismo de Investigación Digital centrado en habilidades de verificación. En octubre de 2016, la Asociación de la Prensa de Madrid (APM) celebró el primer curso de verificación digital presencial específico para periodistas, un curso que se convirtió en referencia y se repitió anualmente hasta el año 2020.

- Muchos medios que publican información de calidad caen en malas prácticas que contribuyen a difundir desinformación de forma involuntaria.

Consejos para evitar estas situaciones:

- Datar imágenes de archivo.
- Transparencia máxima en las fuentes.

- Diferenciar claramente en sus sitios web los formatos de opinión e información.
- Aportar detalles que permitan la trazabilidad de la información.

Cabe reseñar que, en una profesión no regulada en España, los periodistas se rigen por el Código Deontológico de Periodismo, de la FAPE, donde se adquiere el compromiso con la sociedad a mantener en el ejercicio de su profesión los principios éticos y deontológicos que le son propios. En este sentido, existe la Comisión de Arbitraje, Quejas y Deontología del Periodismo[6], también promovida desde FAPE, que se constituye como órgano de autocontrol deontológico interno de la profesión periodística, cuyas resoluciones son interpretadas como una 'sentencia moral', a la que puede dirigirse de forma gratuita cualquier ciudadano que considere que le han sido vulnerados sus derechos, siempre que no haya iniciado acciones judiciales. Sus miembros son profesionales del Derecho, entre los que se encuentran exmagistrados y periodistas de reconocido prestigio.

En el ámbito de Cataluña, existe el Código Deontológico de la profesión periodística del Col·legi de Periodistes de Catalunya[7], desde el año 1992, y el Consell de la Informació de Catalunya, una fundación creada en 1997, impulsada por el mismo colegio, pero de la que forman parte representantes de diferentes instituciones, que tiene el objetivo de ser un órgano de arbitraje privado e independiente que vela por el cumplimiento del citado código. Es un instrumento de autorregulación y sus resoluciones, como en el caso de la Comisión, son de carácter moral.

[6] Más información en https://www.comisiondequejas.com/

[7] Más información en https://fcic.periodistes.cat/

Objeto de la formación

Una asignatura de alfabetización mediática e informacional (AMI) planteada a comienzos de esta tercera década del siglo XXI, debe tener una orientación múltiple, atendiendo a nociones básicas relacionadas con el consumo y la producción de información y con conocimientos de comunicación que favorezcan la expresión y creatividad de los jóvenes y les ayuden a defenderse de toda forma de manipulación. El programa de una posible asignatura debe ser flexible y puede plantearse recuperar los mejores hallazgos de las experiencias nacionales e internacionales anteriores, más significativas. Al mismo tiempo, debe detectar todas las necesidades que se plantean para un uso consciente y crítico de las redes sociales y de los recursos técnicos que se ponen a disposición de los jóvenes en el actual contexto digital. Debe dar a conocer no sólo las bases para un buen uso instrumental de las tecnologías digitales sino también unos principios éticos que partan de la escucha de los jóvenes para poder conocer sus consumos mediáticos, dándoles participación y ayudándoles a pensar con autonomía crítica.

Una asignatura de alfabetización mediática e informacional, planteada a comienzos de la tercera década del siglo XXI, debe tener una orientación múltiple.

Debemos recordar cómo la estrategia de la UNESCO reúne estos dos ámbitos como un conjunto combinado de las competencias (conocimientos, habilidades y actitudes) necesarias para la vida y el trabajo de hoy (Wilson et al., 2011). La AMI abarca todos los tipos de medios de comunicación y otros proveedores de información como bibliotecas, archivos, museos e Internet, independientemente de las tecnologías utilizadas[8].

Estamos en un contexto mediático e informacional en el que es necesario hacer compatibles las enseñanzas sobre el uso y disfrute de medios convencionales (libros, periódicos, radios y canales de televisión), explicando a los jóvenes la importancia de unos medios producidos por profesionales de la información, de la ficción y de la publicidad y otros usos de ocio inteligente derivados de Internet, con acceso a formas de interacción transmedia, desde videojuegos, redes sociales, plataformas digitales y metamedios diversos, que surgen de la evolución de los medios convencionales de información y comunicación.

[8] Más información en http://www.unesco.org/new/es/communication-and-information/media-development/media-literacy/mil-as-composite-concept/

La alfabetización mediática e informacional no puede ser impuesta, debe ser coparticipada y lúdica, partiendo de los gustos e intereses de los propios estudiantes, debatiendo sobre los temas que les motiven, enseñando a ver, a analizar, a producir y dando pistas y orientaciones para un aprovechamiento más creativo de los contenidos mediáticos para un uso inteligente y activo de los mismos. Debe invitar al estudio y motivar al conocimiento, despertando la curiosidad intelectual, invitando a la reflexión y al debate sobre asuntos de actualidad que afectan a la sociedad actual y nos interpelan: defensa del planeta, integración de las minorías, adopción de medidas contra la violencia machista, compensación de las desigualdades, etc.

Ideas para un modelo flexible de formación para abordar la competencia mediática e informacional

1. Autodiagnóstico de la Dieta mediática. Para un autodiagnóstico compartido de consumos:

Partimos de las prácticas de consumo de los y las estudiantes de Bachillerato, con el objetivo de ayudar a promover el necesario diálogo que lleve a implicar a los adolescentes para invitar a su autoanálisis y reflexión sobre los tiempos de consumo, desde libros y periódicos, hasta la exploración de las características de las redes sociales más empleadas y los usos que se hacen de ellas.

¿Qué leemos? ¿Cuánto leemos? ¿Qué redes sociales empleamos, durante qué tiempos, en qué momentos y para qué las empleamos prioritariamente: Whatsapp, Instagram, Tik Tok, Twitter, Facebook, etc.? La pregunta final es, ¿somos conscientes de que, aunque técnicamente sepamos leer y escribir, si no nos ejercitamos somos analfabetos funcionales?

Propuesta Práctica: Identificación de los tiempos de consumo de industrias culturales y redes sociales de cada estudiante. Debate sobre las diferentes formas de consumo de los y las estudiantes.

Identificación de los perfiles de los mediadores en las redes (*influencers, instagramers, youtubers*) y debate sobre las formas de presentación de los contenidos abordados. Invitamos a iniciar una bitácora de la asignatura, individual y propia.

Un primer tema para investigar en la bitácora puede ser, por ejemplo, sobre detección de prácticas de ciberacoso y reflexión para la adopción de medidas que erradiquen esta lacra.

2. ¿Cómo percibimos la realidad? Nuestros sentidos nos engañan. Emoción y razón.

Nociones básicas sobre el sentido de la vista y del oído.

La percepción nos invita a jugar con ilusiones ópticas.

¿Qué nos enseña la teoría de la Gestalt?.

- Pantallas y emociones. Lecciones de la neurociencia aplicadas a situaciones concretas.

Las diferentes metáforas de Joan Ferrés: De la metáfora del Iceberg a la metáfora de la conciliación.

Partir de lo emocional para llegar a la toma de conciencia. Radiografía del receptor y radiografía de la obra. Diagnóstico del receptor y diagnóstico de la obra.

Propuesta práctica: Ponemos en común las preferencias de los integrantes del grupo sobre libros, películas, personajes, preferencias de temáticas y géneros.

Texto inspirador: (Ferrés, 2014)

3. De los medios a las mediaciones. ¿Por qué es importante poder contar con unos medios de información y comunicación hechos por buenos profesionales?

Los valores del Periodismo: Tomamos como referencia los principios definidos por Kovach y Rosenstiel. La importancia de la búsqueda de la verdad, la lealtad a los ciudadanos, la disciplina de verificación, la independencia en relación a aquello de lo que se informa, la independencia del poder, el servir de foro público para la crítica y el comentario, hacer atractiva la información, exhaustividad y proporcionalidad, respeto a la ética y conciencia de los profesionales. (Kovach y Rosenstiel, 2003).

Por qué los jóvenes, al mismo tiempo que cualquier ciudadano, deben acostumbrarse a contrastar fuentes y a oír las diferentes voces para poder tener criterio propio.

Aprendemos a informar en los diferentes medios:

La especificidad de cada medio: medios escritos, medios sonoros, medios audiovisuales y redes sociales.

¿Cómo dar coherencia al relato sobre nosotros mismos?.

Aprender a cuidar nuestra propia imagen y defendernos de la manipulación.

Propuesta práctica: Ponemos en común los principios del periodismo y los aplicamos a temáticas de interés para el grupo. Aprender a comunicar. Prácticas de presentación ante cámara. Identificar bulos y noticias falsas. Formas de manipulación en la imagen y el sonido. Producimos un informativo propio.

Texto inspirador: (Kovach y Rosenstiel, 2003).

4. El lenguaje de la imagen en el contexto digital:

- Del grano de la emulsión al pixel
- Imagen, comunicación y realidad
- Elementos básicos de la imagen
    - La luz.
    - El color.
    - El espacio.
    - El tiempo.
    - El sonido.
    - El texto visual.
- De La realidad construida a la realidad manipulada. De la manipulación de las imágenes analógicas a las *Deep fakes*

Propuesta práctica: Realizamos ejercicios de análisis y producción centrados en cada uno de esos elementos para incorporarlos a la bitácora.

Texto inspirador: (Aparici et al., 2009)

5. La comunicación digital para una alfabetización metamediátca e informacional

- El ciberespacio como no lugar.
- El concepto de metamedios.
- Competencias de producción.
- Competencias de gestión individual y social.
- Competencias performativas.
- Competencias con los medios y las tecnologías.
- Competencias narrativas y estéticas.
- Competencias en la prevención de riesgos, ideología y ética.
- Redes y plataformas: Youtube, Instagram, Wattpad, Facebook.

Propuesta práctica:

Texto inspirador: (Scolari, 2018).

6. Análisis y lectura de la imagen

- Metodologías de análisis de una imagen.
- Del nivel descriptivo al nivel de búsqueda de significado y sentido.
- El valor de saber transmitir en palabras la imagen.
- Pares de características de una imagen.
- Hablan los creadores de imágenes.
- Escenarios virtuales.

Propuesta práctica: En este bloque se procede al análisis sistemático de diferentes tipos de imágenes desde secuencias cinematográficas, spots publicitarios, *selfies*, vídeos volcados en redes sociales, etc.

7. Propuesta de aprendizaje por proyectos y actividades transmedia. Análisis, producción y aprovechamiento social educativo y cultural de medios y metamedios.

- Lenguajes. Ámbito de análisis y ámbito de la expresión
- La tecnología. Ámbito de análisis y ámbito de la expresión
- Procesos de Interacción: ámbito de Análisis y ámbito de la expresión
- Procesos de producción y difusión. Ámbito de análisis y ámbito de la expresión
- Ideología y valores. Ámbito de análisis y ámbito de la expresión
- Estética. Ámbito de análisis y ámbito de la expresión

Propuesta práctica: Producción libre y opcional de diferentes materiales: videoclips, videojuegos, podcast de audio, diseño transmedia, etc.

Texto inspirador: (Ferrés y Piscitelli, 2016)

El perfil de los formadores en alfabetización

Los expertos en comunicación - licenciados, graduados y periodistas - se consideran como el perfil más adecuado en la formación directa a los ciudadanos y/o a los formadores y docentes.

El papel de los verificadores españoles en la alfabetización

Los periodistas dedicados a la verificación en España tienen una visión actual y precisa de la forma en que circula la desinformación en cada momento, ya que trabajan cada día para comprobar la veracidad de esos contenidos.

Los periodistas dedicados a la verificación en España tienen una visión actual y precisa de la forma en que circula la desinformación en cada momento.

Además de identificar los formatos en los que se difunde la desinformación, conocen los canales por los que circula y tienen nociones sobre el impacto de los bulos sobre los usuarios de redes sociales e incluso de redes de mensajería cerrada, ya que las organizaciones de verificación tienen canales de comunicación abiertos con la ciudadanía que les permiten pulsar el estado de la desinformación.

Por estas razones, la participación de los verificadores españoles en las iniciativas de alfabetización digital, y especialmente en las públicas, resulta clave. En la actualidad, sus actividades en este campo se dirigen fundamentalmente a:

- Sensibilización: Explican el problema que plantea la desinformación y cómo identificarla en foros, mesas redondas, vídeos explicativos difundidos en abierto (web o redes sociales), podcast y campañas de sensibilización organizadas en colaboración con instituciones públicas o plataformas digitales.
- Educación: Imparten talleres en abierto (tutoriales en RRSS, en colaboración con ONG) o a medida (a petición de otros medios de comunicación, empresas), títulos propios de especialista o de posgrado (certificados o másteres).

Iniciativas de EFE Verifica

Formación académica

- EFE Verifica imparte cursos y talleres dirigidos a estudiantes de Secundaria y universitarios y a periodistas. La Agencia EFE y la Universidad Carlos III de Madrid (UC3M) ofrecen el Máster de Periodismo de Agencia, una titulación propia que incluye un módulo dedicado a la verificación de datos. EFE Verifica también ha dado talleres sobre *fact-checking* y verificación digital a estudiantes de la Universidad Rey Juan Carlos (URJC) y la UNED. Asimismo, EFE Verifica ha capacitado a periodistas peruanos sobre verificación en elecciones con motivo de los comicios celebrados en 2021.

Producciones audiovisuales

- El equipo de EFE Verifica ha producido vídeos para YouTube, Facebook y Twitter, distribuidos también a través de la red de abonados de la Agencia EFE, en los que se enseña a la audiencia a distinguir mensajes falsos y se habla de la importancia del *fact-checking*.
- También ha asesorado en la producción de este tipo de vídeos a grupos de estudiantes universitarios, como una forma tanto de enseñarles a trabajar en este tipo de formatos como de educarles en la necesidad de adoptar una postura crítica en sus hábitos de consumo mediático.

Concienciación

- EFE ha organizado foros en España y Latinoamérica para concienciar en la necesidad de educar frente a las mal llamadas "noticias falsas", y especialmente en coyunturas críticas por la circulación de desinformación como las elecciones. Así, en colaboración con el Programa de las Naciones Unidas para el Desarrollo (PNUD) y la Unión Europea ha reunido a expertos en desinformación en Brasil, Perú y Paraguay para explicar qué efectos tienen los mensajes desinformativos en la coyuntura electoral y cómo identificarlos y combatirlos.
- En España, EFE Verifica ha organizado foros en colaboración con la UCJC para promover la alfabetización mediática y el consumo de información de calidad, especialmente en un momento de "infodemia" por la circulación de bulos relacionados con el coronavirus.

- El equipo de *fact-checking* de la Agencia EFE también ha participado en jornadas donde ha abordado el problema de la desinformación y ha defendido introducir formación para educar en el consumo de medios y el uso de las redes sociales, tanto a jóvenes como a colectivos en vulnerabilidad digital. Periodistas de EFE han sido invitados a jornadas organizadas por Casa América, Wikipedia, ONG y otros medios de comunicación para tratar esta cuestión.

Iniciativas de VerificaRTVE

Formación

- Periodistas de RTVE asisten a talleres de verificación desde 2016 (primero Documentación y Programas y después Informativos). Estos cursos se han reproducido internamente siguiendo un programa basado en el primer manual sobre la verificación digital elaborado en España: Redondo, M. (2018). Han servido de modelo para la implantación de otros cursos similares en medios y organizaciones como Antena 3 (ATRESMedia), El Mundo (UNEDISA), Europa Press y APM.
- Sesiones de Verificación para estudiantes del Máster en Periodismo de Televisión impartido por el Instituto de Radio Televisión Española y la URJC[9]

Concienciación

- Colaboración con instituciones sanitarias en la lucha contra la desinformación relacionada con la pandemia y la salud (acuerdos con el Colegio de Médicos de Madrid y con el Consejo General de Colegios Oficiales de Farmacéuticos contra la desinformación sanitaria).
- Participación en foros académicos de verificación (como las Jornadas contra la desinformación organizadas por el Observatorio para la Innovación de los Informativos en la Sociedad Digital (IO2) y la Universidad Autónoma de Barcelona (UAB)).
- Participación en el Congreso de los Diputados en el acto de presentación del informe de la ONG Plan Internacional sobre los

[9] Más información en https://www.urjc.es/component/k2/1138-master-en-periodismo-de-television-rtve-urjc

efectos de la desinformación en niñas adolescentes y mujeres adultas, con motivo del Día Internacional de la Niña (VerificaRTVE, 2021).

Contenidos didácticos

- Vídeo con las claves contra el discurso machista y artículo informativo.
- Consejos de Ciberseguridad para evitar caer en bulos de formato fraude digital o phishing.
- Backup, la serie de investigación sobre delitos digitales.
- Claves para confrontar el discurso negacionista.
- El discurso negacionista del cambio climático - divulgación en el programa Whaat!? de Play Z.
- Q, conspiración en la red, colaboración con Informe Semanal.
- Guerra a la Mentira, documental educativo sobre la desinformación del programa En Portada.

Iniciativas de Maldita.es

Formación

- Completo catálogo de talleres y cursos de entre 20' y 30h. Ha formado a estudiantes, funcionarios, periodistas, público en general.
- Máster con la URJC. Maldita tiene un máster de 60 ECS.

Lista de materiales para trabajar la alfabetización mediática de Maldita Educa:

- La caja de herramientas de verificación: contiene los elementos básicos para que tú mismo puedas comprobar los bulos que te llegan. La caja de herramientas de Maldita.es está dividida en diez secciones temáticas: fotografías, videos, buscadores, búsquedas en RRSS, traducción, archivo, mapas de geolocalización, tiempo atmosférico, extensiones para navegadores y varios.
- Curso para combatir la desinformación en Internet: aprende a verificar en 21 tuits. Microcurso sobre *fact-checking* desarrollado en Twitter durante una semana. Divertido, ágil y fácil de seguir. También en inglés.

- Fichas didácticas - Fichas pensadas para trabajar con alumnado de secundaria en educación formal e informal.
    - Qué es la desinformación: La ficha tiene como objetivos definir qué es la desinformación, analizar sus distintas motivaciones y desarrollar el pensamiento crítico:
    - Cómo identificamos la desinformación: La ficha tiene como objetivos identificar a los distintos formatos en que podemos encontrarnos con desinformación y entender que el acceso a la información veraz es un derecho fundamental.
- Fichas con ejercicios de verificación pensadas para jóvenes y adultos.
- Maldita APP - La primera aplicación móvil capaz de avisarte cuando entras con una web con desinformación. Con la app de *Maldita.es* recibirás una notificación cada vez que entres en un contenido que haya desmentido nuestro equipo o en una web que desinforme de manera habitual.
- El Comecocos de Maldita - Juego para descargar e imprimir doblándolo en formato comecocos.
- Verdad o bulo - Juego de cartas para descargar e imprimir. El juego recopila las verdades y desinformaciones alrededor del virus, para que el verificador que todos llevamos dentro aprenda a destaparlos.
- Cómic *Héctor Hecho no comparte bulos*: el cómic trae 7 consejos para que no te la cuelen con ninguna desinformación. Leyendo el tebeo puedes aprender de manera divertida qué hacer cuando te llega un video sospechoso o un pantallazo con contenido turbio, entre otros contenidos.
- Vídeos de material de formación de Maldita Educa en Instagram:
    - Verificar Twitter.
    - Búsqueda inversa de imágenes.
    - Verificar vídeos.
    - Evitar timos online·
    - Qué tener en cuenta al leer un estudio científico.
- Cómo detectar promociones falsas.
- Manual para que no te la cuelen, vídeo.

- No More Haters ¡Rompe la cadena del odio!" tiene como objetivo promover la reflexión y prevenir manifestaciones de odio e intolerancia entre adolescentes y jóvenes de 14 a 29 años. No more hateres es una web-app que se puede descargar en las principales plataformas como Google Play y también se puede jugar desde la web. Está disponible en castellano y en inglés y viene acompañada de una guía docente para que el profesorado pueda trabajar estos temas en el aula. El proyecto incluye también una investigación sobre las actitudes y las experiencias de adolescentes y jóvenes sobre los discursos de odio en la red.
- *Stickers* (pegatinas) para WhatsApp - Pegatinas para desmentir con humor.
- Infografías:
    - Los diez personajes de la desinformación.
    - Cómo se amplifica la desinformación.
    - No digas *Fake news*.
    - ¿Por qué las personas procesamos la información de distintas formas·
    - Qué son y qué no son los *deepfakes*.
    - Cinco consejos para que tu cerebro no te la cuele.
    - Cómo detectar si un tuit es falso.
    - 7 pasos para identificar la desinformación.
    - 7 tipos de desinformación.
    - Manual para luchar contra los bulos.
    - Vigila tus datos.

INICIATIVAS DE MEDIOS GENERALISTAS Y LOCALES, ORGANIZACIONES E INSTITUCIONES POR LA ALFABETIZACIÓN MEDIÁTICA

Las organizaciones profesionales

El Col•legi de Periodistes de Catalunya realiza desde el año 2009 el programa "Premsa a les escoles" con el apoyo de la Obra Social "La Caixa". Se trata de unos talleres, de entre 60 y 90 minutos de duración, impartidos por periodistas colegiados. En su última edición llegó a más de 3.600 alumnos de educación secundaria de 70 centros escolares de Cataluña. El Col•legi, con la financiación de Barcelona Activa, ha iniciado en 2021 unos talleres dirigidos a personas de la tercera edad que se imparten en las bibliotecas municipales de Barcelona.

El Colexio Profesional de Xornalistas de Galicia desarrolla el programa Xornalismo na Escola dirigido anualmente al alumnado de ESO de centros educativos públicos de toda la comunidad. Este programa ha llegado a la quinta edición. A parte de otros programas específicos, el Colexio tiene dos redactados, presentados y pendientes de financiación. El primero de estos programas (en principio piloto), para centros de La Coruña, se denomina Obradoiro de Xornalismo en Igualdade (taller de periodismo en igualdad). Y el otro, que buscará la formación específica de los profesionales en materia de género, está pendiente de la aprobación definitiva por parte de la Xunta de Galicia para empezar a realizarse antes de que finalice el año 2021.

En Andalucía ha habido varias iniciativas promovidas por distintas asociaciones de la prensa (Cádiz, Jerez de la Frontera, Málaga y Sevilla), pertenecientes a la FAPE. Asimismo, a instancias de la federación, las asociaciones organizadas por comunidades autónomas trabajan con las consejerías de educación y otras instituciones, desde diputaciones a ayuntamientos, con el fin de llevar a cabo acciones de alfabetización, no solo en centros de formación, sino también en ámbitos como

Las asociaciones organizadas por comunidades autónomas trabajan con las consejerías de educación y otras instituciones, desde diputaciones a ayuntamientos, con el fin de llevar a cabo acciones de alfabetización.

centros de mayores o asociaciones diversas que integran a diferentes colectivos, entre otros.

La Asociación de la Prensa de Cádiz realizó, entre 2014 y 2018, cinco ediciones del programa 'Periodismo en las aulas', en el que participaron 24.975 alumnos, de 60 centros. Previamente, entre 2010 y 2013, había impartido talleres dentro de un proyecto para dar a conocer la promulgación del IX Decreto de Libertad de Imprenta (1810) y de Libertad de Prensa en la 1a Constitución Española (1812), en los que participaron 3.690 alumnos de 25 centros. La APC también ha impulsado proyectos específicos en materia de tratamiento mediático de la inmigración, como los talleres impulsados desde la Revista de la Asociación, entre 2016 y 2018, y el programa "Y tú ¿por qué te vas' (2019-20), y en materia de género, como el 'Yo periodista', con cinco ediciones (2017-21) de charlas sobre el tratamiento mediático de la mujer.

La Asociación de la Prensa de Jerez (APJ) realiza el proyecto de alfabetización mediática "La Llave Maestra de la Comunicación", en centros educativos desde el curso académico 2013-2014 hasta la actualidad. En este periodo ha recibido aportaciones de la Junta de Andalucía, la Diputación Provincial de Cádiz y La Caixa. Han participado 11.740 alumnos de 92 centros educativos. Puntualmente, la APJ también ha impartido estos talleres a entidades, colectivos y ONG.

"La prensa en mi mochila" es un proyecto didáctico elaborado por la Asociación de la Prensa de Málaga (APM) iniciado en el curso 2018/19. La iniciativa, no solo está destinada al alumnado, sino que también se trabaja con docentes y familias. Una de las características que tiene el proyecto, es que la mayor parte de los centros participantes se encuentran en zonas de exclusión social.

La Asociación de la Prensa de Sevilla (APS) realiza el programa "La Prensa en las escuelas" desde el curso académico 2010/2011. El proyecto, que cuenta desde su inicio con la financiación de la Fundación 'La Caixa', se desarrolló de forma más amplia entre los años 2013 y 2018 gracias a las subvenciones concedidas, mediante concurso público, por la Dirección General de Comunicación Social de la Junta de Andalucía. Han participado 24.940 alumnos de 92 centros.

La Asociación de la Prensa de Madrid lleva a cabo el programa de talleres de 'Fomento de la lectura de la prensa en la escuela', también patrocinado por La Caixa, y que desde 2009 ha llegado a 18.500 escolares, de entre 13 y 17 años, de 82 centros. Este proyecto ganó en 2020 el Premio Nacional de Fomento de la Lectura, que otorga el ministerio de Cultura y Deportes.

Otras organizaciones

El CAC, en colaboración con el Departament d'Educació de la Generalitat de Catalunya, tiene el programa Educac. Ofrece materiales didácticos para el profesorado, con recursos pedagógicos y formación/información, contenidos y propuestas para familias relacionados con el consumo de audiovisuales e internet por parte de niños y adolescentes y convoca anualmente los 'Premios CAC a l'escola'.

En Cataluña existen iniciativas privadas que se dedican a la educación mediática como "Junior Report", "Learn to check", algunas más dirigidas al colectivo de profesores como "Aula Media" y una que se centra en la verificación "Verificat".

También hay radios municipales y televisiones locales que tienen iniciativas muy consolidadas de educación mediática con las escuelas de sus municipios, es el caso de Ràdio Sant Vicenç (Sant Vicenç dels Horts) o Televisió de Badalona, entre muchas otras.

Redes sociales

Enfoque e iniciativas de Facebook sobre alfabetización mediática en España

Contribuir a la alfabetización mediática es un aspecto crucial del enfoque de Facebook para luchar contra la difusión de la desinformación. Para esta compañía, la alfabetización mediática ayuda a las personas a comprender mejor los contenidos que consumen y a tomar decisiones más informadas sobre lo que quieren confiar y compartir. Esto, a su vez, permite a las personas participar en los aspectos económicos, sociales y culturales de la sociedad, así como desempeñar un papel activo en el proceso democrático.

La alfabetización mediática ayuda a las personas a comprender mejor los contenidos que consumen y a tomar decisiones más informadas sobre lo que quieren confiar y compartir.

El enfoque de la alfabetización mediática de Facebook se centra en la colaboración. Se asocian con expertos de la industria, como verificadores de datos, periodistas, ONG y académicos, para

crear programas basados en evidencias que lleguen al público allí donde se encuentre de diversas maneras, tanto en línea como en persona.

Cuentan con un enfoque de la alfabetización mediática basado en el contexto. Sus iniciativas de alfabetización mediática están diseñadas para abordar situaciones específicas que pueden dar lugar a crisis de información, como el voto en las elecciones o el acceso a la vacuna COVID-19. También adoptan un enfoque adaptado para crear iniciativas dirigidas a las necesidades de las comunidades vulnerables. Por ejemplo, tienen socios y programas de apoyo que se centran en las necesidades específicas de las personas mayores, los jóvenes y las comunidades minoritarias.

En la compañía se muestran confiados en el impacto de aprovechar el poder de la tecnología a través de las plataformas de Facebook para hacer que la alfabetización mediática sea más inclusiva y accesible para más personas. Desde 2019, han colaborado con expertos en alfabetización mediática para llevar a cabo campañas de anuncios en Facebook e Instagram que proporcionan a los usuarios consejos sobre cómo detectar la posible desinformación. Esta campaña animaba a las personas a detectar la desinformación comprobando lo siguiente al ver contenidos en línea:

- Comprueba la fuente: Examinar el contenido, incluso si parece tener una base científica.

- Comprueba cómo le hace sentir: las noticias falsas pueden manipular los sentimientos para conseguir clics.

- Comprueba el contexto: busque a las autoridades de salud pública para confirmar el contenido.

Junto con la campaña, realizan un estudio para examinar la eficacia de su enfoque. Hasta la fecha, las campañas han llegado a millones de personas en toda Europa, Oriente Medio y África, con resultados prometedores. En España, la campaña llegó a 11,3 millones de usuarios. A través del texto de efectividad comprobaron un aumento positivo de 7,8 puntos porcentuales en los usuarios que recuerdan activamente haber visto los anuncios y un aumento de 3,1 puntos porcentuales en los usuarios que informan de un cambio de comportamiento después de interactuar con la campaña. El porcentaje de mejora indica la diferencia entre el grupo de prueba y el de control. Utilizarán estos resultados para seguir invirtiendo en iniciativas de alfabetización mediática basadas en pruebas en España.

Asimismo, en España lanzaron GeneraZion, un programa educativo sobre seguridad en Internet y alfabetización mediática para jóvenes que incluye formaciones en colegios y contenidos educativos interactivos en su plataforma digital. En su segunda edición GeneraZion ha llegado a 15.000 estudiantes en formaciones directas en 200 colegios y a 75.000 más en la plataforma digital.

Iniciativas de Google para fomentar la alfabetización mediática

- La alianza contra la desinformación, junto con CLABE (Club Abierto de Editores) y ARI (Asociación de Revistas). A través de estas entidades, Google hace trainings a periodistas para que aprendan las últimas técnicas para verificar y contrastar la información y que, con ello, puedan hacer mejor periodismo.
- La campaña de 'Vacúnate contra los bulos' con Newtral, que cada semana repasa los bulos más sonados y los desmonta. Los vídeos se pueden encontrar en YouTube, Twitter, Instagram y también se hacen directos en Twitch.
- El programa en colaboración con la Fundación de Ayuda contra la Drogadicción (FAD) de Infórmate para que los adolescentes de 14 a 16 años aprendan cómo se hace una noticia y con ello sepan detectar cuándo están ante una noticia falsa.

Herramientas accesibles de alfabetización y de apoyo a posibles desarrollos curriculares

CURRÍCULUM ALFAMED DE FORMACIÓN DE PROFESORES EN EDUCACIÓN MEDIÁTICA

Se trata de una iniciativa de la Asociación Iberoamericana ALFAMED, destinado a la formación de profesores en educación mediática. Cuenta con una edición en español presentada en enero de 2021 y otra en portugués, presentada a comienzos de octubre de 2021. Es un útil instrumento para la acción educomunicativa que profundiza en los avances realizados en este tiempo por todas las personas que, desde la Academia han investigado en propuestas curriculares para la educación en competencia mediática e informacional, desde Paulo Freire hasta nuestros días.

(IN)FÓRMATE

(In)fórmate es una Iniciativa de Google, Fundación de Ayuda contra la Drogadicción (FAD) y el Gobierno de España que cuenta con el apoyo de los medios de comunicación. Se trata de un proyecto de formación en el consumo de medios e información online que promueve la alfabetización mediática y el fomento del pensamiento crítico en la población adolescente de 14 a 16 años que está cursando 3ª y 4º de la ESO en centros educativos españoles.

BECRITICAL

La Fundación “la Caixa pone a disposición de todos los centros educativos un programa, denominado, BeCritical, para potenciar la competencia mediática y el pensamiento crítico del alumnado de la ESO, Bachillerato y Ciclos Formativos. BeCritical facilita tres itinerarios formativos, diferenciados por nivel de intensidad, para adaptarse a las circunstancias de la clase. En el primer bloque de contenidos se realiza una “Aproximación a los medios de comunicación, el lenguaje informativo, las fake news, el periodismo”.

BELLINGCAT

Este equipo europeo lleva años impartiendo talleres de verificación digital que van de lo básico a lo más avanzado[10] (investigación con fuentes abiertas u OSINT). También publica estudios de caso con pautas didácticas y dispone de una de las cajas de herramientas más completa para la comprobación de información en Internet.

DEUTSCHE WELLE AKADEMIE

Esta institución ligada a la televisión alemana Deutsche Welle lleva años realizando cursos de alfabetización mediática y digital en países de África, Asia, Latinoamérica y también en Europa. Desde 2016 se centran también en la desinformación y la verificación digital necesaria para combatirla. Su Laboratorio de Innovación también realiza talleres contra la desinformación.

FIRST DRAFT NEWS

El verificador estadounidense First Draft ofrece guías, talleres y cursos gratuitos en español y otros idiomas para formar a internautas y a periodistas contra la desinformación. Dispone de guías básicas[11] para aprender a verificar información encontrada en Internet, a monitorizar redes sociales o a vigilar contenidos difundidos en aplicaciones de mensajería móvil.

Aporta en su web una caja de herramientas[12] para verificar imágenes y contenidos desde el móvil y organiza talleres y *webinars* de verificación en español y en otros idiomas desde su canal de YouTube. Dispone de cursos generales de verificación y de talleres de temas específicos, como los bulos contra las vacunas de la COVID-19, el discurso xenófobo o procesos electorales concretos.

---

[10] Más información en https://www.bellingcat.com/tag/workshops/

[11] https://firstdraftnews.org/training/

[12] https://firstdraft-toolkit.glideapp.io/

UNIÓN EUROPEA DE RADIODIFUSIÓN (UER)

La UER lleva realizando cursos de filtrado y verificación de contenidos en redes sociales desde 2017, con incidencia en los contenidos generados por usuario (UGC). Son abiertos para periodistas de todo el mundo, con descuento para los medios miembro de UER.

#NODESINFORMACIÓN

El Ministerio de Educación y Formación Profesional a través de la Subdirección de Cooperación Territorial e Innovación Educativa ofrece el recurso editorial #NoDESinformación cuyos objetivos generales son dar a conocer el fenómeno de la desinformación y sus consecuencias en el contexto actual de crisis sanitaria originada por la COVID-19 y promover la alfabetización mediática e informacional como una de las medidas para luchar contra la desinformación. Este material está destinado, principalmente, a docentes de Educación Primaria y Secundaria para que sea usado en las aulas.

NEWS LITERACY PROJECT

Organización sin fines lucrativos dedicada a la educación en medios. El Proyecto de Alfabetización Informativa trabaja con educadores y periodistas para dar a los estudiantes las habilidades que necesitan para discernir la realidad de la ficción y saber en qué confiar. NLP ofrece recursos específicos para educadores, como el programa online Checkology (para personas de entre 6 y 12 años) y otros recursos gratuitos para todo tipo de usuarios.

YOUNG REPORTER (BBC TEACH)

BBC Young Reporter es el proyecto de periodismo y medios de comunicación de la BBC que anima a los jóvenes de entre 11 y 18 años a compartir sus historias y hacer oír su voz.

El enlace “Real News” conduce a una formación que pretende ayudar a los estudiantes de secundaria (de 11 a 18 años) a examinar de forma crítica la información que reciben de sitios web, redes sociales, imágenes y datos, y a desarrollar habilidades y métodos que ayuden a determinar qué es real y qué es falso.

MEDIA WISE

Iniciativa “Media Wise” del Instituto Poynter, dirigido a fomentar el consumo crítico de contenidos online entre personas de todas las edades.

OBSERVATORIO EUROPEO DE MEDIOS DIGITALES (EDMO)

El Observatorio Europeo de Medios Digitales[13] (EDMO) engloba a verificadores, expertos e investigadores académicos para impulsar el análisis de la desinformación y la verificación de contenidos audiovisuales en Europa. Liderado por el Instituto Universidad Europea (con sede en Florencia, Italia), cada mes publica un informe sobre las desinformaciones nacionales y transnacionales detectadas por verificadores en diferentes países europeos.

El Observatorio Europeo de Medios Digitales (EDMO) engloba a verificadores, expertos e investigadores académicos para impulsar el análisis de la desinformación y la verificación de contenidos audiovisuales en Europa.

Organiza cursos de formación presenciales y online para periodistas y expertos y apoya la coordinación de actividades académicas europeas contra la desinformación. Respalda además a las autoridades de países europeos en la supervisión de las medidas para impedir la difusión de bulos y desinformaciones. En su página web ofrece un repositorio internacional de publicaciones científicas sobre desinformación y verificación.

PROJECT LOOK SHARP

De Ithaca College, ofrece seminarios web, artículos, material didáctico y formación profesional para profesores de acceso gratuito. El objetivo del proyecto es enseñar conceptos de alfabetización mediática de modo que los maestros que buscan usar los materiales puedan utilizarlos en sus clases.

---

[13] Más información en http://www.edmo.eu/

CRITICAL MEDIA PROJECT (CMP)

Es un recurso web gratuito de alfabetización mediática para educadores y estudiantes (de 8 a 21 años). El CMP pretende contribuir a mejorar el pensamiento crítico y la empatía de los jóvenes proporcionando herramientas para decodificar los contenidos mediáticos y animando a los jóvenes a crear y contar sus propias historias. Otro programa que tiene como misión contribuir a desarrollar el pensamiento crítico de estudiantes de secundaria es el servicio *Thinkalon, de* Connecticut Public Radio and Television.

COMUNICAR. REVISTA CIENTÍFICA DE COMUNICACIÓN Y EDUCACIÓN

Editada por el grupo andaluz del mismo nombre y fundada por el catedrático de la Universidad de Huelva Ignacio Aguaded. Es la publicación mejor valorada a nivel internacional en Comunicación y Educación. Ha publicado cerca de 1.900 artículos vinculados con la educomunicación en sus 28 años de existencia. Toda esa documentación es accesible para poder comprobar las múltiples investigaciones y experiencias realizadas en España y Latinoamérica en este largo período, lo que constituye un inmenso potencial de consulta, inspirador para futuras iniciativas.

Junto a esta publicación, la Revista Aularia, fundada por Enrique Martínez Salanova, otro de los pioneros de la educomunicación en España, presenta una visión centrada en experiencias de Aula, muy sugerentes también para poder encontrar inspiración en una aplicación práctica de la enseñanza de la competencia mediática e informacional en los diferentes niveles educativos desde una perspectiva educomunicativa.

INICIATIVAS REALIZADAS POR LA UNED

Las iniciativas de postgrado promovidas por el profesor Roberto Aparici en la Universidad Nacional de Educación a Distancia han dado lugar a dos Másteres: el Máster de Comunicación y Educación en la Red y el Máster en Periodismo Transmedia en un proyecto con la Agencia EFE.

Muchos de los materiales producidos por la UNED desde el año 1987 hasta el día de hoy son accesibles y han sido pioneros en esta tarea de alfabetización mediática e informacional. (Aparici y García Marín, 2017).

UNIVERSIDAD DE VALLADOLID. CÁTEDRA DE EDUCOMUNICACIÓN Y TECNOLOGÍAS DISRUPTIVAS

El Campus María Zambrano de la Universidad de Valladolid cuenta desde 2021 con la Cátedra de Educomunicación y Tecnologías disruptivas, dirigida por el Catedrático de Educación Alfonso Gutiérrez y con participación de personal investigador de los tres centros: Facultad de Ciencias Sociales, Jurídicas y de la Comunicación, Facultad de Educación y Escuela de Ingeniería Informática, con una orientación interdisciplinar. El Campus de la UVa acogió dos grandes congresos internacionales de Educación en Competencia mediática e informacional en los años 2011 y 2017 y en la actualidad desarrolla una investigación en INTERNÉTICA.

CONCLUSIONES Y RECOMENDACIONES

- Este grupo entiende que es necesario formar a usuarios autónomos y críticos con los medios de comunicación y la amenaza de la desinformación por diferentes canales que, en las últimas décadas, se pueden haber convertido en potenciales productores de mensajes. Por este motivo parece imprescindible incluir la educación mediática como asignatura específica en el currículum académico de Primaria, Secundaria y Bachillerato. Además de incorporar la tecnología en las aulas hay que dotar a los alumnos de conocimientos sobre la repercusión de los mensajes, para prevenir y eliminar discursos de odio y promover una cultura de encuentro, convivencia y paz.

- Los expertos en comunicación - licenciados, graduados y periodistas - se consideran como el perfil más adecuado en la formación directa a los ciudadanos y/o a los formadores y docentes.

- Además, es preciso desarrollar programas específicos con colectivos vulnerables impulsados desde diferentes instituciones, con competencias en materia social, desde ministerios, comunidades autónomas, a diputaciones y ayuntamientos. En definitiva, se trata de proporcionar conocimientos para evitar los efectos de la manipulación de campañas de desinformación y, en línea con el Plan Integral de Cultura de la Seguridad Nacional, concienciar a los ciudadanos sobre la trascendencia del acceso a una información.

- Se solicita al Gobierno la realización de campañas de información a nivel estatal, contando con las organizaciones profesionales, sobre las consecuencias de la desinformación, poniendo en valor el periodismo de calidad como arma fundamental de esta lucha, teniendo en cuenta que una sociedad bien informada es más difícil de manipular. El buen periodismo separa información de opinión, contrasta fuentes, fomenta el debate público y ofrece pluralidad de pensamiento en favor de la calidad democrática y contra la polarización de los discursos de odio tan frecuentes en las redes. Se entiende que la desinformación afecta a los pilares de la democracia.

- Estas campañas, en línea con la extensión de la formación a distintos ámbitos de la sociedad, deben perseguir también el respeto a la

libertad de expresión y a los derechos de los ciudadanos, como a recibir una información veraz, al honor y la intimidad y a la propiedad intelectual en la educación mediática, en tanto que también es emisor de información (además de receptor). Es decir, formar en aspectos básicos de ética y derecho relacionados con la difusión de información.

- En las campañas informativas se recomendará a los ciudadanos que una correcta 'dieta mediática' pasa por el consumo de medios de comunicación, dado que están sujetos a un código deontológico que garantiza la calidad y la veracidad de la información que reciben, subrayando que se sustentan en empresas y profesionales por lo que no son gratuitos, teniendo en cuenta que detrás de una información hay muchas horas de trabajo.

- Se hace un llamamiento a las instituciones públicas a que realicen un ejercicio de mayor transparencia con el fin de mantener una información clara hacia los ciudadanos, sin partidismo, por entender que los huecos de dudas que se pueden plantear en diferentes situaciones son más sencillos de cubrir con bulos y desinformación.

- Este grupo considera que se debe de mantener de manera estable, con el fin de realizar un seguimiento de las posibles acciones que se puedan llevar a cabo en materia de alfabetización mediática.

REFERENCIAS BIBLIOGRÁFICAS

Aguaded, I., Jaramillo-Dent, D. y Delgado-Ponce, A. (Coords.) (2021). *Currículum Alfamed de formación de profesores en educación mediática*. Octaedro Editorial.

Alaphilippe, A., Gizikis, A., Hanot, C., Bontcheva, K. (2019). *Automated tackling of disinformation*. European Parliamentary Research Service (Parlamento Europeo). https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf

Amoedo, A., Vara-Miguel, A., Negredo, S., Moreno, E., y Kuafmann, J. (2021). *Digital News Report España 2021*. https://www.digitalnewsreport.es/2021/infodemia-y-covid-gran-preocupacion-social-por-los-bulos-de-origen-politico/

Aparici, R. (Coord.) (2010*). Educomunicación: más allá del 2.0*. Gedisa.

Aparici, R., Fernández, J., García Mantilla, A., y Osuna Acedo, S. (2009). *La imagen. Análisis y representación de la realidad*. Gedisa.

Aparici, R. y García-Marín, D. (2017). *Comunicar y Educar en el mundo que viene*. Gedisa.

Aparici, R., y García Marín, D., (Coords.). (2019). *La posverdad. Una cartografía de los medios, las redes y la política*. Gedisa

Aparici Marino, R., García Matilla, A., y Valdivia Santiago, M. (1987). *La imagen*. Universidad Nacional de Educación a Distancia (UNED).

Area Moreira, M., Gros Salvat, B., y Marzal García-Quismondo, M.A. (2008). *Alfabetización y tecnologías de la información y la comunicación*. Editorial Síntesis.

Arteaga Martín, F. (15 de septiembre, 2020). La lucha contra la desinformación: un cambio de modelo. *Real Instituto Elcano*. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-arteaga-la-lucha-contra-la-desinformacion-cambio-de-modelo

Ballesteros Guerra, J.C. y Picazo Sánchez, L. (2018). *Las TIC y su influencia en la socialización de adolescentes*. Centro Reina Sofía sobre Adolescencia y Juventud. Fundación de Ayuda contra la Drogadicción (FAD).

Boletín Oficial del Estado (2015). *Orden ECD/65/2015, de 21 de enero, por la que se describen las relaciones entre las competencias, los contenidos y los criterios de evaluación de la educación primaria, la educación secundaria obligatoria y el bachillerato* (BOE núm. 25, de 29 de enero de 2015, 6986-7003). https://www.boe.es/buscar/doc.php?id=BOE-A-2015-738

Boletín Oficial del Estado (2019). *Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobada por el Consejo de Seguridad Nacional* (BOE núm. 292, de 5 de noviembre de 2020, 96673-96680). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-13663

Brashier, N.M. y Schacter, D.L. (2020). Aging in an Era of Fake News. *Current Directions in Psychological Science*, 29(3), 316-323. https://doi.org/10.1177/0963721420915872

Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., y Saavedra, A. (2019). *Students' civic online reasoning: A national portrait.* Stanford History Education Group & Gibson. https://purl.stanford.edu/gf151tb4868

Buckingham, D. (2005). *Educación en medios: Alfabetización, aprendizaje y cultura contemporánea*. Paidós.

Buckingham, D. (2019). La enseñanza mediática en la era de la posverdad: "fake news", sesgo mediático y el reto para la educación en materia de alfabetización mediática y digital. *Cultura y educación,* 31(2), pp.222-231.

Buitrago, A., Navarro, E., y García Matilla, A. (2015). *La educación Mediática y los profesionales de la comunicación*. Gedisa.

Centro Criptológico Nacional. (2019). *Desinformación en el ciberespacio* (CCN-CERT BP/13). https://www.dsn.gob.es/sites/dsn/files/CCN-CERT_BP_13_Desinformaci%C3%B3n%20en%20el%20Ciberespacio.pdf

Comisión Europea. (2018). *La lucha contra la desinformación en línea: un enfoque europeo* (COM(2018) 236 final). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236&from=EN

Comision Europea. (2018b). *A multidimensional approach to disinformation*, pág. 10. https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en.

Comisión Europea. (2020). *Informe sobre las elecciones al Parlamento Europeo de 2019* (COM(2020) 252 final). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020DC0252

Comisión Europea. (2020b). *La lucha contra la desinformación acerca de la COVID-19: contrastando los datos* (JOIN(2020) 8 final). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020JC0008

Comisión Europea. (2020c). *Combatir la desinformación sobre el Coronavirus*. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_es#results-of-working-with-platforms

Comisión Europea. (2020d). *Desinformación: la UE evalúa el Código de buenas prácticas y publica informes de la plataforma sobre desinformación relacionada con el coronavirus*. https://ec.europa.eu/commission/presscorner/detail/es/ip_20_1568

Consejo de la Unión Europea. (2020). *Conclusiones del Consejo sobre la alfabetización mediática en un mundo en constante transformación* (2020/C 193/06). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XG0609(04)&from=EN

EDELMAN. (2021). *Trust Barometer Spain 2021.* https://www.edelman.com.es/TRUST-BAROMETER-SPAIN-2021

Fattori, S. (15 de abril, 2020). COVID-19: In times of a global pandemic, be aware of the right communication feeds. *Tresca Project*. https://trescaproject.eu/2020/04/15/covid-19-in-times-of-a-global-pandemic-be-aware-of-the-right-communication-feeds/

Ferrés, J. y Piscitelli, A. (2012). La competencia mediática: propuesta articulada de dimensiones e indicadores. *Comunicar*, XIX(38), 75-82. https://doi.org/10.3916/C38-2012-02-08

Ferrés, J., Aguaded, I., y García Matilla, A. (2012). La competencia mediática de la ciudadanía española: dificultades y retos. *Revista ICONO 14. Revista Científica De Comunicación Y Tecnologías Emergentes*, 10(3), 23-42. https://doi.org/10.7195/ri14.v10i3.201

Ferrés, J., García Matilla, A., Aguaded, I., Fernández Cavia, J., Figuera, M., y Blanes, M. (2011) Competencia Mediática. Investigación sobre el grado de competencia de la ciudadanía de España. MEC, (ITE) y CAC.

Ferrés, J. (2014). *Las pantallas y el cerebro emocional*. Gedisa.

Foro Nacional de Ciberseguridad. (22 de julio, 2020). Se constituye oficialmente el Foro Nacional de Ciberseguridad. *Foro Nacional de Ciberseguridad*. https://foronacionalciberseguridad.es/index.php/actualidad/3-se-constituye-oficialmente-el-foro-nacional-de-ciberseguridad

Fundéu (s.f.). *Verificación, mejor que fact-checking*. Recuperado el 4 de octubre de 2021 de https://www.fundeu.es/recomendacion/verificacion-mejor-que-fact-checking.

García Matilla, A. (1999). Escuela, televisión y valores democráticos. *Comunicar*, (13), 107-110. https://www.redalyc.org/pdf/158/15801316.pdf

Gartner. (2017). *Top Strategic Predictions for 2018 and Beyond: Pace Yourself, for Sanity´s Sake*. https://www.gartner.com/en/doc/3803530-top-strategic-predictions-for-2018-and-beyond-pace-yourself-for-sanitys-sake

Gottfried, J. y Grieco, E. (23 de octubre, 2018). Younger Americans are better than older Americans at telling factual news statements from opinions. *Pew Research Center*. https://www.pewresearch.org/fact-tank/2018/10/23/younger-americans-are-better-than-older-americans-at-telling-factual-news-statements-from-opinions/

Guess, A., Nagler, J., y Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, 5(1). DOI: 10.1126/sciadv.aau4586

Guess, A.M., Nyhan, B., y Reifler, J. (2020). Exposure to untrustworthy websites in the 2016 US election. *Nat Hum Behav* 4, 472–480. https://doi.org/10.1038/s41562-020-0833-x

Herrero Curiel, E. y la-Rosa Barrolleta, L. (2021). La Alfabetización mediática en secundaria: transversalidad y voluntad. *Cultura, economía y educación: nuevos desafíos en la sociedad digital*, 76-95. https://www.dykinson.com/libros/cultura-economia-y-educacion-nuevos-desafios-en-la-sociedad-digital/9788413775852/

Herrero-Diz, P., Conde-Jiménez, J., Reyes de Cózar, S. (2020). Teens' Motivations to Spread Fake News on WhatsApp. *Social Media + Society,* 6(3). https://doi.org/10.1177/2056305120942879

Iberifier. (17 de mayo, 2021). Iberifier: proyecto de la Unión Europea para un nuevo observatorio de medios digitales y desinformación en España y Portugal. *Observatorio de cibermedios*. https://observatoriocibermedios.upf.edu/iberifier-observatorio-medios-digitales-desinformacion

Instituto Nacional de Estadística. (2020). *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares*. https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=resultados&idp=1254735976608

IPSOS. (2018). *Fake news, filter bubbles, post-truth and trust*. https://www.ipsos.com/sites/default/files/ct/news/documents/2018-09/fake-news-filter-bubbles-post-truth-and-trust.pdf

Kačinová, V. y Sádaba Chalezquer, M.R. (2022). Conceptualización de la competencia mediática como una "competencia aumentada. *Revista Latina De Comunicación Social*, (80), 21-38. https://doi.org/10.4185/RLCS-2022-1514

Kovach, B. y Rosenstiel, T. (2003). *Los elementos del periodismo*. El País.

Lara, T. (2019). *La construcción de la marca personal del periodista*: *del blog a Twitter (2004-2019)* [Tesis doctoral, Universidad Complutense de Madrid]. E-Prints Complutense https://eprints.ucm.es/id/eprint/58754/

Lascuráin, J. (24 de enero, 2020). El océano semántico de las noticias falsas. *Fundeu*. https://www.fundeu.es/blog/el-oceano-semantico-de-las-noticias-falsas/

LOCE. (2002). *Ley Orgánica 10/2002, de 23 de diciembre, de Calidad de la Educación*, BOE núm. 307, de 24 de diciembre de 2002, 45188-45220. https://www.boe.es/buscar/doc.php?id=BOE-A-2002-25037

LOE. (2006). *Ley orgánica 2/2006, de 3 de mayo, de Educación*. BOE núm. 106, de 4 de mayo de 2006. https://www.boe.es/buscar/act.php?id=BOE-A-2006-7899

LOMLOE. (2020). *Ley orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación*. BOE núm.

340, de 30 de diciembre de 2020, 122868-122953. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-17264

McDougall, J., Brites, M.J., Couto, M.J., y Lucas, C. (2019). Alfabetización digital, fake news y educación. *Educación y Cultura*, 31(2), 203-212, https://doi.org/10.1080/11356405.2019.1603632

McDougall, J., Zezulková, M., van Driel, B., y Sternadel, D. (2018). *Teaching media literacy in Europe: evidence of effective school practices in primary and secondary education*. NESET II Analytical Report. Publications Office of the European Union. https://nesetweb.eu/wp-content/uploads/2019/06/AR2_Full_Report_With_identifiers_Teaching-Media-Literacy.pdf

Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información. (2020). *La sociedad en red. Transformación digital en España. Informe anual 2019*. Madrid: Secretaría General Técnica, Centro de Publicaciones. https://doi.org/10.30923/1989-7424-2020

Pérez Tornero, J.M. (2008). La sociedad multipantallas: retos para la alfabetización mediática. *Revista Comunicar*, XVI (31), 15-25 https://www.revistacomunicar.com/verpdf.php?numero=31&articulo=31-2008-03

Pérez Tornero, J.M., Samy Tayie, S., Tejedor, S., y Pulido, C. (2018). ¿Cómo afrontar las noticias falseadas mediante la alfabetización periodística? Estado de la cuestión· *Doxa Comunicación*, 26, 211-235. https://doi.org/10.31921/doxacom.n26a10

Poulin, M.J., Haase, C.M. (2015). Growing to Trust: Evidence That Trust Increases and Sustains Well-Being Across the Life Span. *Social Psychological and Personality Science,* 6(6), 614-621 https://doi.org/10.1177/1948550615574301

Presidencia del Gobierno. (2019). *Estrategia Nacional de Ciberseguridad 2019*.https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Ragiboglu, G. (21 de agosto, 2020). Los mayores de 50 (y no los jóvenes) son quienes más noticias falsas comparten. *The Conversation*. https://theconversation.com/los-mayores-de-50-y-no-los-jovenes-son-quienes-mas-noticias-falsas-comparten-141649

Redondo, M. (2016). Política automatizada. Bots, trols y propaganda digital encubierta en la comunicación internacional. *Asociación de Comunicación*

Política, ACOP papers (5). https://compolitica.com/wp-content/uploads/publicaciones/ACOPPapersN%C2%BA5_Draft.pdf.

Redondo, M. (2018). *Verificación digital: Manual contra bulos y desinformación internacional*, Universitat Oberta de Catalunya.

Rodríguez Canfranc, P., Villar García, J.P., Tarín Quirós, C., y Blázquez Soria, J. (2020). *Sociedad digital en España*. Fundación Telefónica. https://www.fundaciontelefonica.com/cultura-digital/publicaciones/sociedad-digital-en-espana-2019/699/

Rodríguez-Martínez, R., Mauri, M., Ramon, X., Chaparro, M., Egaña, T., Fanals, L., Herrera, S., Morata, M., Moreno Gil, V., Luengo, M., Palà, G., Pérez Pereiro, M., Requejo Alemán, J.L., Rojas Torrijos, J.L., Salgado, F., Suárez, P., Tulloch, C., Zuberogoitia, A. *Desinformación y plataformas de fact-checking: estado de la cuestión*. Serie Editorial FACCTMedia. http://hdl.handle.net/10230/48029

Salaverría, R., Buslón, N., López-Pan, F., León, B., López-Goñi, I., y Erviti, M.-C. (2020). Desinformación en tiempos de pandemia: tipología de los bulos sobre la Covid-19. *Profesional De La Información*, 29(3). https://doi.org/10.3145/epi.2020.may.15

Scolari, C.A. (2018). *Adolescentes, medios de comunicación y culturas colaborativas. Aprovechando las competencias transmedia de los jóvenes en el aula*. EC | H2020 | Research and Innovation Actions.

Skurnik, I., Yoon, C., Park, D.C., y Schwarz, N. (2005). How Warnings about False Claims Become Recommendations. *Journal of Consumer Research,* 31(4). 713-724. https://doi.org/10.1086/426605

Statista (2021). *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025.* https://www.statista.com/statistics/871513/worldwide-data-created/

Toffler, A. (1970). *Future Shock*. Random House.

Tribunal de Cuentas Europeo. (2021). *Informe Especial 09/2021: El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada*. https://www.eca.europa.eu/es/Pages/DocItem.aspx?did=58682

Universidad Carlos III de Madrid. (s.f.). *Cátedra Jean Monnet Chair "EU, Disinformation & Fake News".* https://www.uc3m.es/investigacion/catedras-investigacion/jean-monnet-chair-eu-disinformation-fake-news

VerificaRTVE. (4 de octubre, 2021). Una de cada cuatro jóvenes se siente físicamente inseguras por culpa de la desinformación. *RTVE*. https://www.rtve.es/noticias/20211004/informe-desinformacion-mujeres-jovenes-salud-mental-participacion/2179620.shtml

Wardle, C. (14 de marzo, 2017). Fake news. It's complicated. *First Draft News*. https://firstdraftnews.org/articles/noticias-falsas-es-complicado/

Wardle, C. y Derakhshan, H. (2017). *Information disorder: toward an interdisciplinary framework for research and policymaking* (DGI(2017)09). Consejo de Europa. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Wason, P.C. (1960). On the failure to eliminate hypotheses in a conceptual task. *Quarterly journal of experimental psychology*, 12(3), 129-40. https://doi.org/10.1080/17470216008416717

Wiesehomeier, N. y Flynn, D.J. (noviembre, 2020). ¿Quién se cree las "fake news" en España? *Observatorio Social de Fundación "la Caixa"*. https://elobservatoriosocial.fundacionlacaixa.org/es/-/quien-se-cree-las-fake-news-en-espana?

Wilson, C., Grizzle, A., Tuazon, R., Akyempong, K., y Cheung, C.K. (2011). *Alfabetización Mediática e Informacional Curriculum para profesores*. UNESCO.

Young, O. (s.f.). Misinformation and COVID-19. *Co-inform*. https://coinform.eu/misinformation-and-covid-19/

CAPÍTULO 4

PROPUESTAS PARA COMBATIR LAS CAMPAÑAS DE DESINFORMACIÓN EN PROCESOS ELECTORALES

Coordinador sociedad civil:

Jordi Rodríguez Virgili (Universidad de Navarra)

Coordinador institucional:

Ministerio del Interior - Dirección General de Política Interior

Autores y colaboradores:

Desirée García Pruñonosa (EFE verifica)

Javier Castro-Villacañas (Federación de Asociaciones de Radio y Televisión de España)

Carlos Hernández-Echevarría Monge (Maldita.es)

Guillermo Serrano Peña (Meta)

Gabriel López Serrano (Microsoft)

Yolanda Quintana Serrano (Plataforma en Defensa de la Libertad de Información)

Mira Milosevich Juaristi (Real Instituto Elcano)

Eva Navarrete Maceas (Red de Colegios de Periodistas)

José Barrera Castaño (Red de Colegios de Periodistas)

María de Reparaz de la Serna (Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales)

Camino Rojo Torres (Twitter)

Raúl Magallón Rosa (Universidad Carlos III de Madrid)

Nuria Navarro Sierra (Universidad Rey Juan Carlos)

INTRODUCCIÓN

Considerar la desinformación en materia electoral de manera específica y propia de estudio de un grupo de trabajo ha favorecido un fructífero debate e intercambio de opiniones y conocimientos entre los expertos que lo han integrado. La labor de este grupo no solo ha permitido incluir en el presente documento una batería de recomendaciones y propuestas dirigidas tanto a la sociedad civil como a los actores en el proceso, sino que ha reforzado los lazos entre diversas instancias al objeto de constituir una estructura permanente de colaboración que permita trabajar en la lucha contra la desinformación con ocasión de la convocatoria de un proceso electoral.

Los trabajos se han enriquecido con aportaciones de expertos a los que se ha invitado en calidad de tales y, tanto desde Microsoft como desde Facebook y Twitter, se han presentado ponencias de gran interés. La participación del ámbito académico ha permitido perfilar y contextualizar con mayor rigor las propuestas finales. La experiencia de las agencias de verificación (EFE Verifica y Maldita.es) ha enriquecido de manera sustancial los trabajos y así ha ocurrido también con la representación del sector del periodismo. La parte institucional del grupo de trabajo se ha visto reforzada por la incorporación de un representante de la Junta Electoral Central (JEC). Su participación, inicialmente no prevista, ha enriquecido los debates y precisado las recomendaciones finales.

En cuanto al contenido del informe elaborado, se ha optado por dar la mayor relevancia posible a las propuestas y recomendaciones, no sin antes contextualizar la materia, tanto en el ámbito nacional como internacional, y resumir las principales medidas adoptadas hasta la fecha. De este modo, este capítulo se estructura en dos grandes partes, una expositiva y otra propositiva.

La primera parte recoge, por un lado, el análisis de las experiencias nacionales e internacionales de los últimos años; y por otro, en epígrafe distinto, las medidas que tanto el sector público como el privado ya han puesto en marcha, porque

antes de realizar nuevas propuestas parece relevante sintetizar las respuestas contra la desinformación que ya están aplicando los distintos actores.

La segunda parte, contiene las propuestas y recomendaciones del grupo de trabajo, agrupadas según los destinatarios de las mismas. Así, hay recomendaciones dirigidas a los partidos políticos, a la sociedad civil, a las plataformas, a los medios de comunicación, a la Administración Pública, a la JEC y al Legislador, lo que pone de manifiesto la importancia del trabajo colaborativo de todos los sectores en la lucha contra la desinformación.

Finalmente, cabe destacar que alguna de las medidas que se contienen en el documento ya han comenzado a analizarse en detalle por sus destinatarios para facilitar su implementación lo antes posible.

ANÁLISIS DE CASOS INTERNACIONALES Y NACIONALES

En la actualidad se habla de guerra híbrida o "infoguerra" para referirse a la búsqueda de escenarios alternativos a una guerra convencional –con consecuencias físicas y reales- que afectan a la convivencia diplomática, económica y política entre Estados. Diversos actores políticos (estatales y no estatales) han encontrado en el entorno digital nuevas estrategias de influencia internacional a través de la desinformación.

En este sentido, la desinformación busca atacar infraestructuras críticas de la democracia para obtener ventajas, desestabilizar su funcionamiento o cuestionar su legitimidad. La desinformación mina la confianza en el sistema democrático y sobre todo en los procesos electorales, que son la base sobre la que se construye la democracia moderna. De ahí que las campañas de desinformación se intensifiquen antes y durante los procesos democráticos de toma de decisiones (elecciones, referéndums, etc.).

La desinformación mina la confianza en el sistema democrático y en los procesos electorales, que son la base sobre la que se construye la democracia moderna.

Sin embargo, la respuesta contra estas amenazas no puede venir por el control de la información ni la censura, porque si bien la confianza en el sistema es fundamental para la democracia, no lo es menos que esa confianza se asienta en el control al poder y su rendición de cuentas. Control judicial, parlamentario y social, este último ejercido principalmente por los periodistas, pero con un protagonismo creciente de los ciudadanos a través de las redes sociales. Información y democracia van aparejadas. Cuanto mejor informada está la sociedad, más inmune se hace a los intentos de manipulación.

Se ha comprobado que la desinformación puede tener efectos más pronunciados en contenidos políticos que en temas sobre terrorismo, desastres naturales, ciencia o información financiera (Vosoughi et al., 2018). La desinformación impacta en la construcción de la realidad por parte de los ciudadanos, hasta el punto de influir en su percepción y toma de decisiones, aun a sabiendas de su origen deliberadamente ficticio (de Keersmaecker y Roets, 2017). Sin embargo, la eficacia de la desinformación para alterar resultados electorales es relativa y, de momento, se carece de evidencia científica, empírica y consistente, de la influencia en opiniones, actitudes o comportamientos

políticos de los ciudadanos que se exponen a desinformación. Con todo, esta influencia inmediata sería menos nociva que los efectos estructurales sobre el sistema democrático, porque la desinformación afecta a la raíz de la base de la confianza, que es la legitimidad de los elegidos (Norris et al., 2015; Rubio, 2018).

Casos internacionales

Los casos más paradigmáticos de desinformación conocidos públicamente hasta la fecha se dieron en 2016 tanto en el referéndum del Brexit del Reino Unido (Bennett y Livingston, 2018; Krzyżanowski, 2019) como en las elecciones presidenciales de Estados Unidos (Allcott y Gentzkow, 2017; Guess et al., 2018). Aunque con distinto protagonismo, en ambos casos estuvo involucrada Cambridge Analytica, la empresa que, según se reveló el 17 de marzo de 2018, habría recopilado al menos 50 millones de perfiles usados "para construir un poderoso programa de software para predecir e influir en las urnas" (Cadwalladr y Graham-Harrison, 2018). Desde 2016 se han detectado, con mayor o menor precisión, campañas de desinformación en múltiples procesos electorales de países tan dispares como Francia (Ferrara, 2020), México (Martínez, 2018) o Taiwán (Stanford Internet Observatory, 2020).

Los casos más paradigmáticos de desinformación se dieron en 2016 tanto en el referéndum del Reino Unido como en las elecciones presidenciales de Estados Unidos.

El elemento del perjuicio intencional es crucial en el concepto de desinformación, como recoge el *Grupo de Expertos de Alto Nivel sobre Noticias Falsas y Desinformación* designado por la Comisión Europea al definir la desinformación como "todas las formas de información falsa, inexacta o engañosa diseñada, presentada y promovida para causar daño público intencionadamente o con fines de lucro" (Comisión Europea, 2018). Una información falsa no es ilegal en sí misma, su divulgación debe causar también un perjuicio individual o colectivo. Como señala el Tribunal Europeo de Derechos Humanos (TEDH), no puede limitarse el debate público incluso si existen sospechas de que la

Foto 12: Ilustración sobre Inteligencia Artificial, por Gerd Almann.

información divulgada no sea veraz[1]. Porque en palabras de este mismo tribunal: "las elecciones libres y la libertad de expresión, especialmente la libertad del debate político, constituyen los cimientos de todo régimen democrático"[2]. También el Tribunal Constitucional español mantiene una línea jurisprudencial homogénea en la que su afirmación clave sobre el contenido de la noción "información veraz" es que "lo que ampara el art. 20.1 d) es la información rectamente obtenida y difundida, aun cuando su total exactitud sea controvertible"[3].

Las elecciones libres y la libertad de expresión, especialmente la libertad del debate político, constituyen los cimientos de todo régimen democrático.

Los motivos de quienes emprenden campañas de desinformación en procesos electorales pueden ser muy variados, pero fundamentalmente se agrupan en razones ideológicas, económicas y, sobre todo, geopolíticas.

La motivación ideológica o puramente electoral pretende incidir en el resultado del proceso. Suelen tener su origen en la acción de los partidos políticos o sus entornos, aunque en ocasiones puedan contar con la ayuda de actores externos. Estas campañas resultan más difíciles de someter a la legislación electoral. Como ejemplo de este tipo de motivación pueden mencionarse las elecciones presidenciales de México, marcadas por la estrategia de empleo de *bots* y *trolls* de diferentes candidatos (Magallón, 2019).

Las motivaciones económicas se constataron, por ejemplo, en las elecciones norteamericanas de 2016. Una investigación de la revista Wired (Subramanian, 2017), publicada en febrero de 2017 sobre las granjas de contenidos en Macedonia que habían contaminado el debate público en las elecciones estadounidenses de 2016, ya apuntaba a la cuestión económica por encima de la ideológica para explicar un modelo de negocio que explota la tensión electoral. El 3 de noviembre de 2016, Craig Silverman y Lawrence Alexander publicaban en Buzzfeed una investigación titulada "Cómo unos adolescentes en los Balcanes están engañando a los partidarios de Donald Trump con noticias falsas" (Silverman y Alexander, 2016) en la que identificaban más de 100 sitios web pro-Trump que se localizaban desde una sola ciudad en la ex República Yugoslava de Macedonia, Veles, con 45.000 habitantes.

---

[1] STEDH, caso Handyside contra Reino Unido, de 7 de diciembre de 1976.

[2] STEDH, caso Bowman, de 19 de febrero de 1998, Párr. 42, y STEDH, caso Mathieu-Mohin y Clerfayt, de 2 marzo 1987, Párr. 47.

[3] STC 121/2002, de 20 de mayo 2002.

Las motivaciones geopolíticas buscan desestabilizar la democracia o provocar una reacción desproporcionada que cuestione el carácter democrático del país afectado. Tratan de introducir el virus de la duda en el proceso, debilitar la legitimidad del gobernante elegido independientemente de quién sea. Se ha comprobado de formas diversas y con diversa intensidad en, por ejemplo, las acusaciones de Donald Trump sobre un supuesto fraude electoral en Estados Unidos de 2020 o en la primera vuelta de las elecciones presidenciales de Ecuador, donde se introdujeron dudas sobre el recuento (BBC News Mundo, 2021).

En las campañas de desinformación con motivación geopolítica suelen estar involucrados terceros países (Torres Soriano, 2017). Ejemplo de ello fue, una vez más, la ya mencionada elección norteamericana de 2016 (Hall Jamieson, 2018). En octubre de 2017, Facebook comunicó que una compañía vinculada al Kremlin llamada Internet Research Agency -ubicada en San Petersburgo- había realizado hasta 80.000 publicaciones en su plataforma entre enero de 2015 y agosto de 2017 que fueron expuestas a una cifra inicial de 29 millones de usuarios estadounidenses[4].

Estas campañas de desinformación con motivaciones geopolíticas se extendieron a otros países y procesos electorales. Así, en 2017, la campaña del candidato presidencial francés Emmanuel Macron fue víctima de varios ciberataques lanzados por hackers vinculados a Rusia (Hacquebord, 2017). Un estudio publicado en 2019 por el Oxford Internet Institute menciona que "un puñado de actores estatales sofisticados usan propaganda computacional para operaciones de influencia extranjera. Facebook y Twitter atribuyeron operaciones de influencia extranjera a siete países (China, India, Irán, Pakistán, Rusia, Arabia Saudita y Venezuela) que han utilizado estas plataformas para influir en audiencias globales" (Bradshaw y Howard, 2019).

En las campañas de desinformación con motivación geopolítica suelen estar involucrados terceros países.

El problema de la desinformación no sólo tiene que ver con la fabricación de informaciones falsas sino también con la forma en que se distribuyen. El alcance y uso de los sistemas de mensajería en la circulación y distribución de

[4] "Hasta 126 millones de usuarios de Facebook podrían haber visualizado contenido producido y difundido por agentes rusos. Por su parte, Twitter declaró que había descubierto 2.752 cuentas controladas por rusos, y que más de 36.000 bots rusos produjeron 1,4 millones de tuits durante las elecciones. Finalmente, Google reveló que había encontrado en Youtube 1.108 videos con 43 horas de contenido relacionado con la injerencia rusa" (Puig, 2017).

la desinformación depende de cada país y, por lo tanto, los patrones globales se tienen que poner en relación a los contextos locales que determinan su uso comunicativo. El informe del Reuters Institute de 2018 señalaba que los sistemas de mensajería se estaban convirtiendo en la principal fuente de circulación de rumores y bulos. Estas herramientas de mensajería instantánea son redes encriptadas y, por tanto, no es fácil saber qué información se está compartiendo y qué tipo de mensajes circulan por los grupos de carácter político. Para Nic Newman, coautor del informe, "las razones por las que las personas se están mudando a estos espacios es porque obtienen más privacidad. Si estás en un régimen autoritario, puedes usarlo para hablar con seguridad sobre política, pero también puede usarse para medios nefastos" (Newman et al., 2018).

Los sistemas de mensajería se estaban convirtiendo en la principal fuente de circulación de rumores y bulos.

De una forma u otra, los países democráticos han reaccionado contra estas campañas de desinformación, incluyendo la actualización de propuestas legislativas o normativas aprobadas sobre publicidad electoral como ha sido el caso de EEUU[5], Nueva Zelanda[6] o diferentes países de la Unión Europea (Furnémont y Kevin, 2020). En Canadá se prohibió la "Influencia indebida por parte de extranjeros" tanto en el proceso de votación como en la financiación de las campañas[7]. Incluso en Taiwán se han adoptado medidas directas contra la injerencia de la República Popular China como la prohibición de determinadas plataformas mediáticas chinas, como iQIYI (la plataforma de video de Baidu) y Tencent video, en el mercado taiwanés o la Ley de Medios de Comunicación Públicos, que abordó la gobernanza de las juntas, la rendición de cuentas y la independencia financiera de los grupos de medios de comunicación (Dickey, 2019).

Los países democráticos han reaccionado contra estas campañas de desinformación, incluyendo la actualización de propuestas legislativas o normativas aprobadas sobre publicidad electoral.

También la Unión Europea decidió crear un grupo de expertos para el análisis de las *fake news* y la desinformación. Más adelante se detallarán algunas de las medidas adoptadas en el marco de la UE para combatir la desinformación en

[5] Véase: https://www.congress.gov/bill/115th-congress/senate-bill/1989/text

[6] Véase: https://elections.nz/guidance-and-rules/for-voters/about-election-advertising/

[7] Véase Elections Modernization Act https://www.elections.ca/content.aspx?section=med&dir=-c76&document=index&lang=e

los procesos electorales. En este escenario, Andrus Ansip, vicepresidente responsable del Mercado Único Digital, señalaba:

> "La desinformación, como instrumento de influencia política, no es ninguna novedad. Las nuevas tecnologías, especialmente las digitales, han ampliado su alcance a través del entorno en línea para socavar nuestra democracia y nuestra sociedad. Puesto que la confianza en línea es fácil de romper y difícil de recuperar, el sector necesita colaborar con nosotros en esta cuestión. Las plataformas en línea desempeñan un papel importante en la lucha contra las campañas de desinformación organizadas por personas y países que quieren poner en peligro nuestra democracia"[8].

En diciembre de 2018 la UE, presentó un plan de acción para intensificar los esfuerzos para contrarrestar la desinformación tanto en Europa como fuera de la UE. Andrus Ansip, señalaba:

> "Debemos estar juntos y aunar fuerzas para proteger nuestras democracias frente a la desinformación. Hemos observado tentativas de interferir en las elecciones y referéndums, y las pruebas apuntan a Rusia como principal fuente de esas campañas. Para hacer frente a estas amenazas, proponemos mejorar la coordinación con los Estados miembros a través de un sistema de alerta rápida, reforzar nuestros equipos dedicados a desenmascarar la desinformación, aumentar el apoyo a los medios de comunicación y a los investigadores e instar a las plataformas online a cumplir sus compromisos. Luchar contra la desinformación requiere un esfuerzo colectivo"[9].

---

[8] Véase: https://twitter.com/ansip_eu/status/989435708065579008

[9] Véase : https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6647

Casos nacionales

Las elecciones de nuestro país también se han visto afectadas por la desinformación (Paniagua et al., 2020). EFE Verifica y Maldita.es han analizado la naturaleza de las desinformaciones más viralizadas en Internet (unos 30 ejemplos) durante las tres convocatorias electorales más recientes en España: las elecciones generales de noviembre de 2019, las elecciones al Parlament de Catalunya de febrero de 2021 y las elecciones a la Asamblea de Madrid del mismo año (véase Anexo 1).

La mayor parte de los contenidos desinformadores difundidos durante estas convocatorias electorales entraron dentro de la categoría de contenido fabricado (100% falso, diseñado para engañar y dañar), contenido engañoso (uso engañoso de información para incriminar a alguien o algo), o contenido manipulado (manipulación de información o imágenes genuinas para engañar), según la clasificación de Claire Wardle, cofundadora y directora de First Draft (Wardle, 2017).

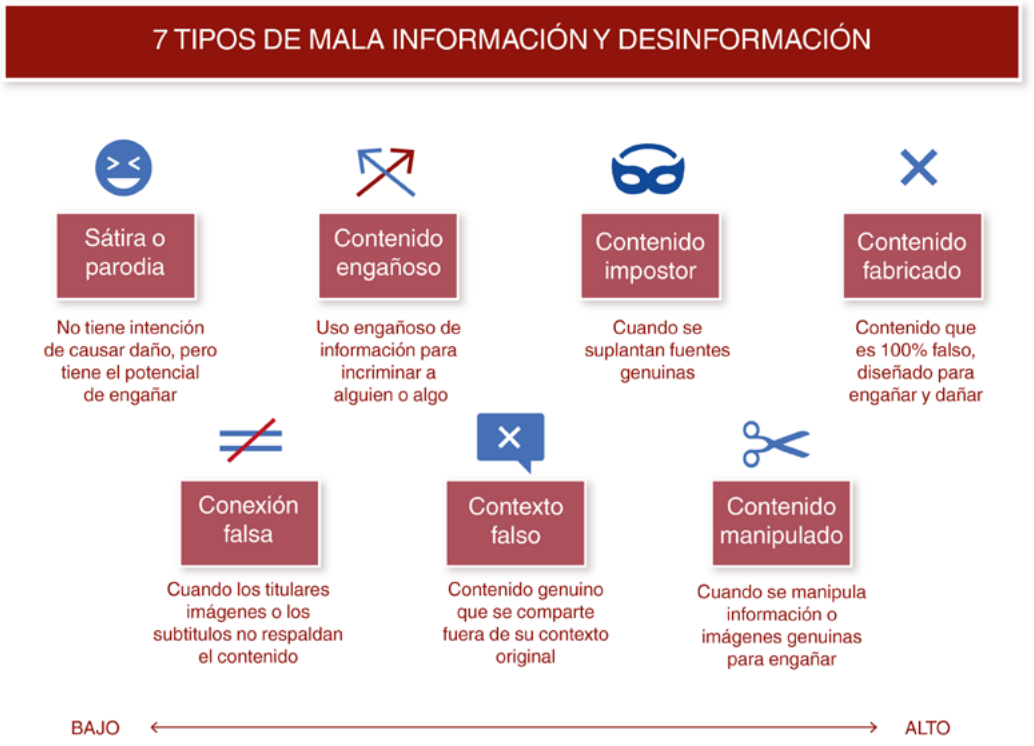


Gráfico 6: 7 Tipos de malainformación y desinformación
Fuente: Wardle, 2017. Traducido por el DSN

Respecto a los tipos de contenidos generados por los usuarios (CGU) con los que se ha intentado engañar o manipular en los últimos procesos electorales en España, en la mayoría de ocasiones se trata de textos publicados en tuits, sistemas de mensajería instantánea o redes sociales, pero también capturas de pantalla de esos mismos contenidos. Aparecen además notas de voz y vídeos y fotos manipuladas o fuera de contexto.

La motivación del bulo está relacionada siempre con la política, y casi siempre se dirige a desacreditar al gobierno, a un partido político o candidato y/o a la integridad y fiabilidad del propio sistema electoral. Los ataques a la limpieza del recuento de votos han ido incrementándose en los últimos años; tradicionalmente se había acusado a las compañías que proveen de sistemas tecnológicos para el escrutinio en España de interferir en el recuento electoral, un bulo que sigue circulando cada vez que hay elecciones. También surgen una y otra vez bulos relacionados que denuncian sin pruebas una supuesta manipulación del voto por correo.

Además de la desinformación contra los contendientes electorales o contra el propio proceso, durante el período anterior a los comicios suele aparecer otra que vincula esas dos categorías con el ataque a colectivos vulnerables, acusando sin pruebas a inmigrantes de votar de forma irregular.

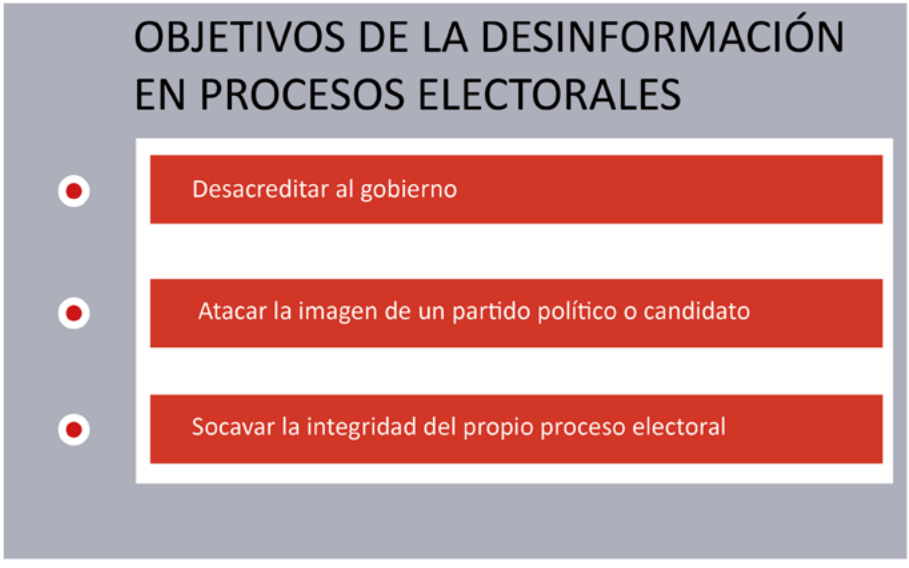


Gráfico 7: Objetivos de la desinformación en procesos electorales
Elaborado por el DSN

MEDIDAS ADOPTADAS POR EL SECTOR PÚBLICO Y PRIVADO

Ante las amenazas de estas campañas de desinformación en España, el sector público y privado han reaccionado con la toma de distintas decisiones, que conviene recordar antes de sugerir nuevas respuestas.

Sector público

Marco Europeo

La Comisión Europea ha manifestado que la desinformación perjudica a nuestra sociedad porque erosiona la confianza en las instituciones y los medios de comunicación, pone en peligro las elecciones, obstaculiza la capacidad de los ciudadanos para tomar decisiones con conocimiento de causa y la máxima información veraz posible y menoscaba su libertad de expresión.

A continuación, se sintetizan las medidas adoptadas en el marco de la UE relacionadas con desinformación en el marco de los procesos electorales y que contextualizan la creación de la Red de coordinación para la seguridad de los procesos electorales en el ámbito de la competencia de la Administración General del Estado en España.

Propuestas de la Comisión Europea para unas elecciones europeas libres y seguras, de 12 de septiembre de 2018 (Comisión Europea, 2018b).

Con el objetivo de hacer frente a las posibles amenazas a las elecciones y reforzar así la resistencia de los sistemas democráticos de la Unión, la Comisión propuso una serie de actuaciones para proteger mejor los procesos democráticos de la manipulación por parte de terceros países o de intereses privados:

1. Recomendación sobre las redes de cooperación electoral, la transparencia en línea, la protección contra los incidentes de ciberseguridad y la lucha contra las campañas de desinformación: Se anima a los Estados

miembros a crear una red nacional de cooperación electoral formada por las autoridades pertinentes -como las electorales, las de ciberseguridad, las de protección de datos y las policiales- y a designar un punto de contacto para participar en una red de cooperación electoral a nivel europeo. Esto permitirá a las autoridades detectar rápidamente posibles amenazas, intercambiar información y garantizar una respuesta rápida y bien coordinada.

2. Recomendación sobre la necesidad de una mayor transparencia en la publicidad política en línea y en la selección de objetivos.

3. Las autoridades nacionales, los partidos políticos y los medios de comunicación deben tomar medidas para proteger sus redes y sistemas de información de las amenazas de ciberseguridad, basándose en las orientaciones elaboradas por las autoridades nacionales en el marco del grupo de cooperación sobre redes y sistemas de información (NIS), con la Agencia de Ciberseguridad de la UE y la Comisión Europea.

4. Orientaciones sobre la aplicación de la legislación de la UE en materia de protección de datos. La Comisión recuerda las obligaciones de protección de datos para todos los actores en las elecciones europeas.

5. Modificación legislativa para endurecer las normas de financiación de los partidos políticos europeos.

6. Un Reglamento para poner en común los recursos y la experiencia en tecnología de ciberseguridad. Para hacer frente a la constante evolución de las ciberamenazas, la Comisión propone crear una Red de Centros de Competencia de Ciberseguridad para orientar y coordinar mejor la financiación disponible para la cooperación, la investigación y la innovación en materia de ciberseguridad. Un nuevo Centro Europeo de Competencia en Ciberseguridad gestionará la ayuda financiera relacionada con la ciberseguridad con cargo al presupuesto de la UE y facilitará la inversión conjunta de la Unión, los Estados miembros y la industria para impulsar la industria de la ciberseguridad de la UE y garantizar que nuestros sistemas de defensa sean punteros.

Código de buenas prácticas de 8 de octubre de 2018 (Comisión Europea, 2018c).

Se trata de un compromiso de distintos agentes y actores privados para fijar unas normas de autorregulación para luchar contra la desinformación y que recoge un variado y nutrido número de medidas concretas.

El Código fue firmado por las plataformas en línea Facebook, Google, Twitter y Mozilla, así como por los anunciantes y parte de la industria publicitaria en octubre de 2018. Microsoft se unió en mayo de 2019, y TikTok en junio de 2020. En la actualidad, la Comisión Europea quiere reforzar y mejorar este código de buenas prácticas (Comisión Europea, 2021).

Plan de Acción de la Unión Europea contra la desinformación de 5 de diciembre de 2018 (Comisión Europea, 2018d).

A instancias del Consejo Europeo, y con origen en los trabajos de un grupo de expertos de alto nivel en el seno de la Comisión encargado de asesorar sobre la lucha contra la desinformación, la Comisión presenta el Plan de Acción de la Unión Europea contra la desinformación, entre cuyas acciones previstas (un total de diez) se encuentra la aplicación efectiva del conjunto de medidas concebidas para garantizar unas elecciones europeas libres y justas teniendo presente que estas se celebrarían en 2019.

El Plan incluye la propuesta de que los Estados miembros designen puntos nacionales de contacto que participen en el Sistema de Alerta Rápida (RAS), que facilite el conocimiento compartido y la respuesta coordinada cuando en un Estado miembro se atente contra la democracia y que se sustenta en una plataforma digital segura para que los Estados miembros intercambien información y se adopten medidas coordinadas de actuación en casos de desinformación.

Comisión Especial del Parlamento sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión (junio 2020)[10]

Tiene como objetivo evaluar las investigaciones que apuntan a la vulneración de la legislación electoral y a las operaciones auspiciadas desde el extranjero, con el objetivo de identificar medidas en redes sociales como parte de una estrategia coordinada frente a las amenazas híbridas y contrarrestar campañas de comunicación desde terceros países.

Informe sobre el balance de las elecciones europeas (Parlamento Europeo, 2020)

En su Considerando Y, el informe señala que "los procesos democráticos, tanto a escala de Estados miembros como europea, han sido el blanco de potencias extranjeras, a veces en conexión con agentes internos, que buscaban influir en el resultado de las elecciones y debilitar a la Unión" y que "los mecanismos puestos en marcha por la Unión, como el Código de Buenas Prácticas en materia de Desinformación o el sistema de alerta rápida en relación con las elecciones, han contribuido a mitigar las injerencias extranjeras durante la campaña electoral".

El informe dedica sus puntos 23 y 24 a la desinformación, señalando la necesidad de una actuación conjunta más potente y un refuerzo de la educación cívica. El punto 24 señala que "la injerencia ilegítima en los procesos electorales no es un fenómeno de origen exclusivamente exterior" y "estima que los algoritmos que proporcionan contenidos en las plataformas de medios sociales deben ser objeto de supervisión y, en caso necesario, de regulación, con el fin de garantizar que la información a la que tienen acceso los ciudadanos no está sesgada y que se protege su derecho a la información durante y después de las campañas electorales".

Finalmente, en su apartado 26 insta a la Comisión y al Consejo a tomar medidas para "luchar contra la injerencia exterior y las dimensiones interna y externa de manera efectiva" y a colaborar con la nueva Comisión Especial del Parlamento sobre injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la Desinformación (INGE).

---

[10] Véase: https://www.europarl.europa.eu/committees/es/inge/home/highlights

Marco nacional español

Red de coordinación en materia de seguridad de procesos electorales en el ámbito de la Administración General del Estado.

Como la coordinación de los Estados miembros de la Unión es esencial, tal y como ya se ha señalado, la Comisión Europea propuso en su Recomendación de 12 de septiembre de 2018 un conjunto de medidas con vistas a "reducir los riesgos en las próximas elecciones" (Comisión Europea, 2018b).

En su Recomendación, la Comisión Europea determina que "cada Estado Miembro debe crear una Red Nacional en materia de elecciones, en la que participen las autoridades nacionales con competencias en el ámbito electoral y las autoridades responsables del seguimiento y la aplicación de las normas relativas a las actividades en línea que pueden incidir en el contexto electoral […]", de ese modo podrán detectar rápidamente las amenazas potenciales a las elecciones al Parlamento Europeo y hacer cumplir rápidamente las normas vigentes, incluso mediante la imposición de sanciones.

Foto 13: Apoderados de distintos partidos controlan el recuento de votos tras el cierre de los colegios en las elecciones autonómicas de Madrid de 2021. EFE/David Fernández

Si bien esta propuesta de la Comisión se incardina en las elecciones al Parlamento Europeo, por la concurrencia y el uso conjunto de medios, la incidencia y la alineación de sus objetivos, parece innegable su aplicación al resto de procesos en los que hay una participación directa del ciudadano.

La Red de Coordinación para la Seguridad en Procesos Electorales (la Red) en el ámbito de la competencia de la Administración General del Estado viene a reforzar la resiliencia en periodos de elecciones o en aquellos procesos en las que hay participación directa del ciudadano, estableciendo medidas equilibradas, globales y específicas encaminadas a respaldar la integridad y una organización eficaz de los procesos en los que la competencia esté atribuida a la Administración General del Estado, como una responsabilidad conjunta de todos los agentes que participan en dicho proceso.

La Red de Coordinación para la Seguridad en Procesos Electorales en el ámbito de la competencia de la Administración General del Estado viene a reforzar la resiliencia en periodos de elecciones.

Para la consecución del objetivo señalado, y con el objeto de integrar esta red nacional dentro de la Red Europea de Seguridad en Elecciones surgida de la Comunicación adoptada por la Comisión Europea sobre cómo garantizar elecciones libres y justas, las acciones que desarrolla la Red se estructuran en cuatro grandes bloques:

- Garantizar que el proceso electoral se lleve a cabo con transparencia y objetividad y acorde con el principio de igualdad, respetando las reglas del juego previstas en el procedimiento electoral.
- Proteger contra la utilización indebida de datos personales.
- Establecer procedimientos frente al riesgo que representan los ciberataques para los sistemas informáticos de las elecciones, las campañas, los partidos políticos, los candidatos o las administraciones públicas, velando por la seguridad de todos los aspectos informáticos del proceso electoral.
- Combatir la desinformación en línea y las noticias falsas.

De este modo, y para atender cada uno de ellos, la Red integra a las siguientes instituciones y organismos:

Tal y como se recoge en el gráfico, los cuatro pilares sobre los que trabaja la Red y los organismos e instituciones vinculados a cada uno de ellos son:

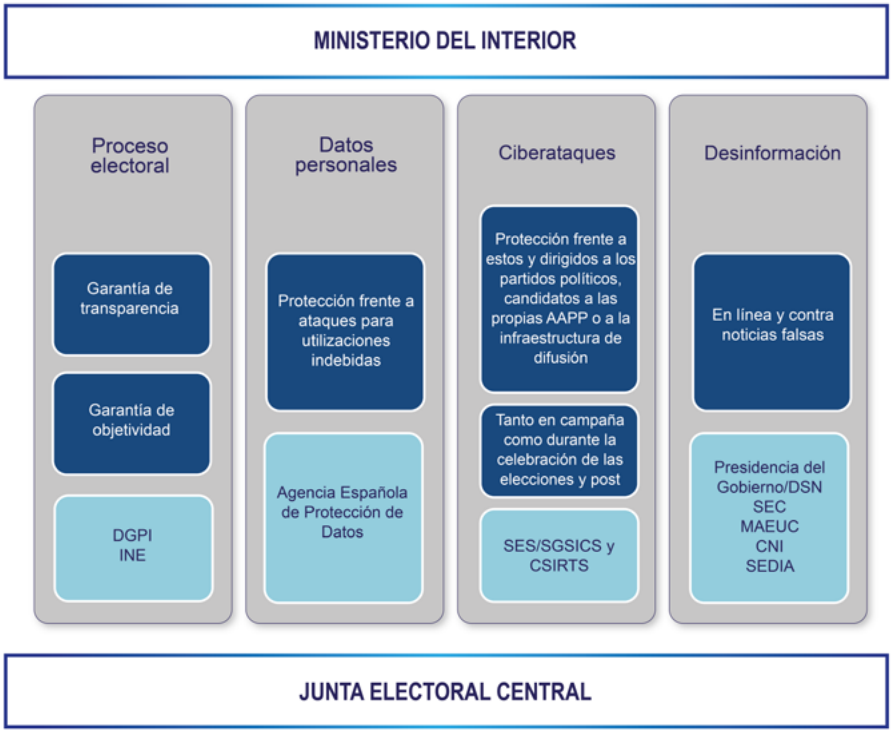


Gráfico 8: La Red de Coordinación para la Seguridad en Procesos Electorales (La Red)
Fuente Ministerio del Interior

- Proceso electoral. Con la finalidad de proteger los principios de transparencia y objetividad, los miembros de la Red encargados de esta tarea son tanto el Ministerio del Interior (a través de la Dirección General de Política Interior) como el Instituto Nacional de Estadística.
- Datos personales. Con la finalidad de protección frente a ataques para utilizaciones indebidas de estos. El miembro de la Red vinculado con este pilar es la Agencia Española de Protección de Datos.

- Ciberataques. Con la finalidad de proteger frente a estos y teniendo en cuenta también los ataques dirigidos a partidos políticos, candidatos, a las propias Administraciones Públicas o a la infraestructura de difusión de resultados; y ello tanto en campaña como durante la celebración de las elecciones e incluso posteriormente. Los organismos vinculados a este pilar son la Subdirección General de Sistemas de la Información y Comunicaciones, el Centro Nacional de Protección de Infraestructuras y Ciberseguridad y el Equipo de Respuesta ante Incidencias de Seguridad Informáticas (todos ellos del Ministerio del Interior).
- Desinformación. Con la finalidad de detectar y actuar contra las falsas noticias y campañas de desinformación, los organismos de la Red vinculados a este pilar son el Departamento de Seguridad Nacional (DSN) y Secretaría de Estado de Comunicación (SEC) de Presidencia del Gobierno, el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación (Dirección General de Comunicación, Diplomacia Pública y Redes), Ministerio de Defensa (Centro Nacional de Inteligencia -CNI-) y Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Transformación Digital e Inteligencia Artificial -SEDIA-).

Con carácter horizontal y actuación y supervisión de los cuatro pilares se encuentra el Ministerio del Interior, por su competencia en materia de procesos electorales, y la JEC, como vértice de la pirámide de la Administración Electoral.

La Red se puso en marcha en 2019 para atender no solo las elecciones al Parlamento Europeo de mayo de 2019 que concurrieron con las elecciones autonómicas y locales, sino también con ocasión de las elecciones a Cortes Generales de abril y de noviembre del mismo año.

El trabajo colaborativo y coordinado de todos los organismos que forman parte de la Red permitió dar respuesta rápida a algunas incidencias detectadas, como la caída de algunas webs institucionales, así como la detección de diversas actuaciones que podrían enmarcarse en el ámbito de la desinformación, pero cuya relevancia finalmente no se consideró de la entidad suficiente como para poner en marcha acción alguna.

La Red demostró ser una herramienta útil y de necesaria vocación de permanencia. Asimismo, en el marco de la propuesta tercera de la Recomendación de septiembre de 2018, la protección de las infraestructuras electorales, pese a no tener éstas carácter permanente, gozan de una condición equivalente a la de las infraestructuras críticas dada su condición de “servicio esencial”.

Sector privado

La conversación pública se ha digitalizado. La aparición de Internet, las plataformas de mensajería y las redes sociales han dado al fenómeno de la desinformación, tan antiguo como la comunicación, un nuevo protagonismo. La universalización de herramientas de difusión como las redes sociales, su inmediatez, alto alcance potencial, facilidad de uso y su carácter gratuito multiplica la capacidad de comunicación, pero también la divulgación de la desinformación.

La aparición de Internet, las plataformas de mensajería y las redes sociales han dado al fenómeno de la desinformación, tan antiguo como la comunicación, un nuevo protagonismo.

Esta desinformación en contextos digitales evoluciona con perfiles y grupos falsos en redes sociales, publicidad engañosa y *clickbait*, *bots* y *trolls*, inteligencia artificial y *deepfakes*, que pretenden influir en los comportamientos y las decisiones electorales de la ciudadanía (Alaphilippe et al., 2019). En consecuencia, las plataformas sociales y tecnológicas han actualizado sus políticas para combatir las campañas de desinformación. A continuación, se resumen las medidas más importantes tomadas por las plataformas tecnológicas y redes sociales que, por su influencia o penetración, tienen mayor protagonismo en las elecciones en España: Twitter y Facebook.

Twitter

Twitter se presenta como una plataforma que ha permitido que personas de todo el mundo expresen libremente su opinión y considera que ha sido un factor catalizador en la movilización de diversos movimientos sociales, piedras angulares del cambio social. El propósito de Twitter y el resto de plataformas sociales de servir a la conversación pública es ahora más crítico que nunca.

En concreto, esta empresa tecnológica defiende que las personas que usan la plataforma deben tener el contexto adecuado en torno a la información engañosa para poder decidir por sí mismos la veracidad de la información y, al mismo tiempo, evitar la propagación de contenido que pueda provocar daños fuera del ecosistema digital.

A continuación, se detallan algunas de las medidas que Twitter ha adoptado para intentar proteger y fomentar una conversación pública saludable.

1. *Política relativa a la información engañosa sobre la COVID-19*[11]. En el contexto de una pandemia mundial, la información errónea sobre las vacunas ha presentado todo un desafío de salud pública. La plataforma afirma estar enfocada a mitigar la información engañosa que presenta el mayor daño potencial para la salud y el bienestar de las personas. Estas experiencias podrían extrapolarse a combatir las campañas de desinformación en procesos electorales. Por ejemplo, bajo su política actual, Twitter puede exigir la eliminación de los tuits que incluyan información falsa o engañosa sobre la COVID-19[12].

   También puede etiquetar o colocar una advertencia en los tuits que presenten rumores sin fundamento, afirmaciones en disputa, así como información incompleta o fuera de contexto sobre las vacunas. Los tuits que están etiquetados bajo esta guía ampliada pueden vincularse a información de salud pública autorizada o las Reglas de Twitter para proporcionar a las personas contexto adicional e información autorizada sobre COVID-19[13].

   Aviso proactivo en la plataforma[14]. En febrero de 2020, en colaboración con el Ministerio de Sanidad, se lanzó un aviso proactivo que dirige a los usuarios a información autorizada por el Ministerio sobre la COVID-19. De esta manera, Twitter pretende asegurarse de que sus usuarios tienen acceso a información fidedigna y de fuentes autorizadas cuando busquen #COVID19, #coronavirus #vacuna y otros términos de activación relacionados en Twitter. Como se ha comentado, se trata de actuaciones que pueden ser extrapoladas a la materia electoral.

2. *Política de integridad cívica*[15]. Formalmente Twitter prohíbe los intentos de utilizar sus servicios para manipular o interrumpir procesos cívicos, incluso mediante la distribución de información falsa o engañosa sobre los procedimientos o circunstancias relativos a la participación en un proceso cívico. En los casos en que se use

---

[11] Véase https://help.twitter.com/es/rules-and-policies/medical-misinformation-polic

[12] Algunos ejemplos pueden encontrarse en: https://help.twitter.com/es/rules-and-policies/medical-misinformation-policy

[13] https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information

[14] https://twitter.com/Policy/status/1222581255574827008

[15] Véase https://help.twitter.com/es/rules-and-policies/election-integrity-policy

información engañosa que no pretenda manipular o interrumpir directamente procesos cívicos, pero que genere confusión respecto de su servicio, puede etiquetar los tuits para brindar contexto adicional.

Las consecuencias de incumplir la política de integridad cívica varían según la gravedad, el tipo de incumplimiento y los antecedentes de incumplimiento de la cuenta infractora. En los casos en que las cuentas incumplan repetidamente esta política, la empresa usa un sistema de advertencia para determinar si se deben considerar otras acciones de control de cumplimiento. Desde la plataforma, se señala que este sistema ayuda aún más a reducir la difusión de información errónea potencialmente dañina y engañosa en Twitter, especialmente cuando se trata de incumplimientos graves de las reglas de la plataforma. Ejemplos de las medidas que pueden tomar: eliminación del Tweet, modificaciones del perfil, etiquetas o bloqueos y suspensión permanente de la cuenta.

Twitter también dispone de etiquetas para que no haya dudas de cuándo se interactúa con una cuenta oficial de gobierno o de medios afiliados a un Estado[16]. Pretenden ofrecer más contexto cuando se necesita.

Como parte de sus políticas, Twitter usa etiquetas para agregar contexto a afirmaciones engañosas y también reduce la visibilidad de estos tuits a fin de mitigar posibles daños. Además, a través de su política relativa a los contenidos multimedia falsos y alterados[17], agrega etiquetas al contenido que promueve, con la intención de engañar, contenidos multimedia falsos o alterados.

3. *La Política relativa al spam y la manipulación de la plataforma* establece que no se pueden usar los servicios de Twitter con el propósito de amplificar o suprimir información de forma artificial, ni llevar a cabo acciones que manipulen u obstaculicen la experiencia de los usuarios[18]. Formalmente, no se permite el *spam* ni ningún otro tipo de manipulación de la plataforma. Manipular la plataforma es usar Twitter para llevar a cabo acciones masivas, de alta intensidad

[16] https://help.twitter.com/es/rules-and-policies/state-affiliated

[17] https://help.twitter.com/es/rules-and-policies/manipulated-media

[18] https://help.twitter.com/es/rules-and-policies/platform-manipulation

o engañosas que confunden a los usuarios o que obstaculizan su experiencia. Hay muchas formas de manipular la plataforma, y las reglas de Twitter están focalizadas en intentar contrarrestar una gran variedad de comportamientos prohibidos[19].

Además, en septiembre de 2021, Twitter anunció que está probando una función de etiquetado que permitirá que las cuentas automatizadas (conocidas como *bots*) se identifiquen a sí mismas para mejorar la experiencia de los usuarios[20].

4. *Campañas de Alfabetización Mediática*. Además del trabajo de Twitter que se materializa en productos, políticas y cumplimiento de sus reglas, la plataforma también fomenta la alfabetización mediática.

   En asociación con la UNESCO, Twitter ha lanzado el manual de alfabetización mediática *Enseñar y aprender con Twitter*[21]. Junto a socios locales como PantallasAmigas, Maldita.es, Al fanar o Plan Internacional España, Twitter pretende ayudar a equipar a las generaciones más jóvenes con habilidades de alfabetización mediática, permitiéndoles hacer las preguntas correctas sobre el contenido con el que interactúan en Twitter y analizar críticamente las noticias y las informaciones que reciben online.

   Recientemente, la plataforma ha lanzado un proyecto piloto llamado *Birdwatch*[22] para probar soluciones basadas en la comunidad para información engañosa y actualmente está recopilando datos sobre su uso entre un grupo seleccionado de usuarios (por el momento, solo en EEUU).

   Twitter también afirma trabajar con socios y expertos de confianza en diversos mercados para entender el contexto local, la cultura y matices. Su Consejo de Confianza y Seguridad les informa sobre las tendencias recientes e importantes en una variedad de temas[23].

---

[19] Pueden verse algunos ejemplos en https://help.twitter.com/es/rules-and-policies/platform-manipulation

[20] Véase https://help.twitter.com/es/using-twitter/automated-account-labels

[21] Véase https://en.unesco.org/sites/default/files/gmw2019_twitter_mil_guide_es.pdf

[22] Véase https://blog.twitter.com/en_us/topics/product/2021/introducing-birdwatch-a-community-based-approach-to-misinformation.html

[23] Véase https://about.twitter.com/en/our-priorities/healthy-conversations/trust-and-safety-council

El Consejo de Confianza y Seguridad de Twitter es un grupo de organizaciones de expertos independientes de todo el mundo, que asesoran a la plataforma a medida que ésta desarrolla sus productos, programas y reglas.

Las áreas de enfoque incluyen seguridad y acoso en línea, derechos humanos y digitales, prevención del suicidio y salud mental, explotación sexual infantil y deshumanización.

Además, con carácter general, Twitter puede brindar formación y otorgar *AdsForGood* (crédito publicitario pro bono) para apoyar los esfuerzos y actividades de la sociedad civil en la plataforma.

5. *Operaciones de Información*. Siguiendo los principios de transparencia -y con el fin de mejorar la comprensión del público sobre las supuestas campañas de influencia no auténticas-, esta empresa tecnológica publica archivos relativos a tuits y contenidos multimedia que considera que provienen de operaciones de información que están vinculadas con ciertos Estados y que han tenido lugar en su servicio.

   En octubre de 2018, presentó el primer archivo sobre operaciones de información extranjeras potenciales observadas en su red social. Su opinión fundamental es que estas cuentas deberían ser públicas y permitir búsquedas a fin de que miembros del público, gobiernos e investigadores puedan investigar, aprender y desarrollar conocimientos multimedia para el futuro. La compañía ha ampliado este conjunto de datos con varias actualizaciones durante los últimos dos años. Además, está adquiriendo, desarrollando y creando un enfoque tecnológico impulsado por su personal para intentar hacer frente a las campañas de influencia no auténticas[24].

6. En 2019, Twitter actualizó su *Política de Contenido de Carácter Político*[25]. Esta política se aplica a los productos publicitarios de pago. Twitter prohíbe en todo el mundo la promoción de contenido de carácter político.

---

[24] El archivo de Twitter de Operaciones de Información está disponible en https://transparency.twitter.com/es_es/reports/information-operations.html

[25] Véase https://business.twitter.com/es/help/ads-policies/ads-content-policies/political-content.html

La plataforma define el contenido de carácter político como aquel que hace referencia a un candidato, partido político, funcionario gubernamental electo o designado, elección, referéndum, medida sometida a votación, ley, normativa, directiva o fallo judicial. Los anuncios que contengan referencias a contenido de carácter político, incluidas peticiones de votos, solicitudes de apoyo financiero y promoción a favor o en contra de los tipos de contenido de carácter político mencionados anteriormente, quedan prohibidos en virtud de esta política. Tampoco están permitidos anuncios de ningún tipo de parte de candidatos, partidos políticos o funcionarios del gobierno elegidos o designados.

7. *Acerca de las excepciones de interés público en Twitter*[26]. Por lo general, la compañía toma medidas sobre los tuits que incumplen sus reglas. Sin embargo, reconoce que a veces puede servir al interés público permitir que las personas vean tuits que, en circunstancias normales, se eliminarían. Twitter considera que el contenido es de interés público si constituye un aporte directo para la comprensión o el debate de un asunto que preocupa a todo el público. En la actualidad, la plataforma limita estas excepciones a un tipo crítico: tuits de funcionarios electos y del gobierno, dada la importancia del interés público en conocer y poder debatir sus acciones y declaraciones.

   Como resultado, en casos excepcionales, la plataforma puede optar por conservar un tuit de un cargo electo o del gobierno que, de lo contrario, se eliminaría. En su lugar, lo colocará detrás de un aviso que proporcione un contexto sobre el incumplimiento de las reglas y que permitirá que las personas hagan clic para ver el Tweet. Colocar un tuit detrás de este aviso también pretende limitar la capacidad de interactuar con el tuit a través de “Me gusta”, “Retuits”, o de compartirlo en Twitter, y busca asegurar que el algoritmo de la red social no lo recomiende. El objetivo de estas acciones es intentar limitar el alcance del tuit sin afectar la capacidad del público para verlo y debatirlo.

[26] Véase https://help.twitter.com/es/rules-and-policies/public-interest

Los criterios y procesos mediante los cuales la plataforma decide si un Tweet, que de otra forma incumpliría las Reglas de Twitter, es de interés público, son los siguientes:

1. El tuit incumple una o más de las Reglas de Twitter[27];
2. El autor del tuit es una cuenta verificada;
3. La cuenta tiene más de 100.000 seguidores; y
4. La cuenta representa a un miembro actual o potencial de un organismo gubernamental o legislativo local, estatal, nacional o supranacional:
    - titulares actuales de un puesto de liderazgo elegido o designado en un organismo gubernamental o legislativo,
    - candidatos o nominados para cargos políticos, o
    - partidos políticos registrados.

La excepción de interés público no significa que cualquier funcionario público o cargo electo que cumple con los criterios puede tuitear lo que quiera sin importar si incumple las Reglas de Twitter. Para decidir si debe eliminar un tuit o colocarlo detrás de un aviso, Twitter considera el posible riesgo y la gravedad del daño y lo compara con el valor para el interés público del tuit. Cuando el riesgo de daño es mayor o más grave, es menos probable que haga una excepción.

Para decidir si debe eliminar un tuit o colocarlo detrás de un aviso, Twitter considera el posible riesgo y la gravedad del daño y lo compara con el valor para el interés público del tuit.

Es más probable que aplique el aviso a un tuit que comete un incumplimiento si:

- El tuit está dirigido a otros funcionarios del gobierno o cargos electos o instituciones como parte de un debate público o llamado a protestar.
- El tuit es relevante para el rol público del autor o del objetivo.
- El tuit proporciona un contexto importante para los eventos o problemas geopolíticos en curso.

[27] Véase https://help.twitter.com/es/rules-and-policies/twitter-rules

- O existe un importante valor documental o de responsabilidad en la preservación del contenido, como un asunto de registro público.

Es más probable que Twitter elimine el tuit sin aplicar el aviso si:

- El tuit incluye una llamada a la acción declarativa que podría dañar a una persona o un grupo de personas específico.
- En el tuit se comparte información o se participa en un comportamiento que podría interferir directamente con el ejercicio de los derechos fundamentales de una persona[28].

Facebook

Desde Facebook se señala que proteger la integridad de las elecciones al tiempo que se preserva la libertad de expresión es una prioridad. Teniendo en cuenta las lecciones del pasado y las aportaciones de expertos y responsables políticos de todo el espectro político, la compañía afirma haber invertido en equipos y tecnologías para mejorar la seguridad de las elecciones y defiende que las despliega allí donde considera que tendrán el mayor impacto. Facebook habría estado presente en más de 200 elecciones en todo el mundo desde 2017, y ha creado nuevos productos y desarrollado políticas más sólidas para prepararse ante futuras elecciones.

Facebook ha creado nuevos productos y desarrollado políticas más sólidas para prepararse ante futuras elecciones.

La plataforma tiene más de 35.000 personas trabajando en seguridad en todo el mundo. Su labor consiste en vigilar la actividad sospechosa, identificar rápidamente los contenidos y comportamientos que infringen las políticas de la compañía, eliminarlos y evitar que se vuelvan a utilizar. Facebook cuenta con 40 equipos involucrados en este trabajo y más de 500 personas dedicadas exclusivamente a las elecciones. La estrategia para proteger las elecciones no sólo se aplicaría durante los momentos críticos, sino durante todo el año, y se centraría en tres áreas:

- Eliminar los contenidos perjudiciales y reducir la desinformación
- Impedir las injerencias
- Aumentar la transparencia y el control de los usuarios

[28] Más información sobre cuándo es más o menos probable que Twitter haga excepciones en https://help.twitter.com/es/rules-and-policies/public-interest

Nota preliminar sobre la terminología que usa Facebook

En el debate sobre la desinformación hay mucha confusión entre conceptos como desinformación, información falsa o errónea, injerencia extranjera, operaciones de influencia/información e incluso integridad electoral.

Facebook utiliza el término desinformación para referirse a las afirmaciones que son engañosas o falsas. Por otro lado, usa el término operaciones de influencia para describir las acciones coordinadas que tienen como objetivo manipular o corromper el debate público con un objetivo estratégico. Dos indicadores clave de las Operaciones de Influencia (OI) son la inautenticidad y la coordinación.

Desde la red social señalan que la distinción entre desinformación y operaciones de influencia es importante, porque las preocupaciones políticas que subyacen a cada una de ellas son diferentes, y la respuesta más adecuada de plataformas como Facebook también será diferente. Una diferencia fundamental en la forma de abordar la desinformación y las OI es que Facebook distingue entre ambas en función del actor/comportamiento y del contenido. En el caso de las OI, se centra en los actores y su comportamiento, mientras que en el caso de la desinformación lo hacen en el contenido.

1. *Eliminar contenidos perjudiciales y reducir la desinformación*

Facebook aplica una estrategia basada en tres pilares -eliminar, reducir e informar- para abordar el contenido problemático en toda la familia de aplicaciones de la plataforma[29]. Esto implica eliminar el contenido que infrinja las políticas de Facebook, reducir la difusión del contenido problemático que no infringe sus políticas pero que aun así socava la autenticidad de la plataforma, e informar a las personas con información adicional para que puedan elegir dónde hacer clic, qué leer o compartir.

Asimismo, Facebook defiende que se muestra comprometido con esfuerzos de autorregulación que abarcan los tres elementos de esta estrategia, como el Código de Prácticas de la UE sobre Desinformación. Según la plataforma, el Código es una herramienta ágil y novedosa que se lanzó en las elecciones al Parlamento Europeo de 2019 y que se ha convertido en un activo en la lucha contra la desinformación sobre la COVID-19. Con base en las orientaciones de la Comisión Europea (mayo de 2021) Facebook afirma trabajar con los demás signatarios en una versión actualizada del Código, reforzada con definiciones,

[29] Véase https://transparency.fb.com/es-es/features/approach-to-misinformation/

una mayor transparencia y cooperación con las comunidades de investigación y *fact-checking*.

Se detalla a continuación cómo se aplican los tres pilares al contenido problemático.

a. Eliminar:

Facebook elimina el contenido que viola las Normas de la Comunidad[30]:

- Cuentas falsas[31] y cuentas con comportamientos no auténticos[32]. Desde Facebook señalan que se han desactivado más de un millón de cuentas falsas al día en el momento de su creación.
- La desinformación que pueda contribuir a un riesgo de violencia o daño inminente[33].
- Fraude o injerencia en el voto, lo que incluye cualquier tergiversación sobre cómo participar en el proceso de votación como las fechas, el lugar, la hora, los métodos y la calificación[34].
- Anuncios que infrinjan las Políticas de Publicidad[35], incluidos los anuncios con afirmaciones desacreditadas por *fact-checkers* o, en ciertas circunstancias, por organismos autorizados (como la OMS en el ámbito de la COVID-19), así como las Normas de la Comunidad.

Desde el comienzo de la pandemia, desde la plataforma se indica que se han eliminado más de 20 millones de casos de desinformación sobre la COVID-19 tanto en Facebook como en Instagram.

---

[30] Véasehttps://transparency.fb.com/es-es/policies/community-standards/?from=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2F

[31] Véase https://transparency.fb.com/data/community-standards-enforcement/?from=https%3A%2F%2Ftransparency.facebook.com%2Fcommunity-standards-enforcement#fake-accounts

[32] Véase https://transparency.fb.com/es-es/policies/community-standards/inauthentic-behavior/?from=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Finauthentic_behavior

[33] Véase https://transparency.fb.com/es-es/policies/community-standards/violence-incitement/?from=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fcredible_violence

[34] Véase https://transparency.fb.com/es-es/policies/community-standards/coordinating-harm-publicizing-crime/?from=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fcoordinating_harm_publicizing_crime

[35] Véase https://www.facebook.com/policies/ads

b. Reducir:

Para contenido problemático que no incumple las Normas de la Comunidad pero que socava la autenticidad de la plataforma como el *clickbait* y el contenido desacreditado por verificadores independientes[36], Facebook señala que reduce su presencia en la sección de noticias. Para aumentar la transparencia en este trabajo, la compañía lanzó públicamente las Directrices de Distribución de Contenidos (CDG), que explican qué contenido recibe una distribución reducida en Facebook porque es problemático o de baja calidad[37].

Estos criterios y decisiones de clasificación señalan que se desarrollaron en colaboración con una comunidad global y de expertos externos. De esta manera, cuando un contenido es degradado se reduce significativamente el número de personas en Facebook e Instagram que lo ven.

Para esta tarea, Facebook confía en la colaboración con verificadores independientes. Mantiene una colaboración global con la International Fact-checking Network (IFCN) y colabora con *fact-checkers* certificados por la IFCN. Facebook trabaja con más de 80 organizaciones independientes de verificadores en 60 idiomas en todo el mundo para revisar y calificar la precisión del contenido en la plataforma. En España colabora con EFE Verifica, Newtral, Maldita y AFP, todas ellas acreditadas por la IFCN.

El enfoque se centra en identificar el contenido que debe ser revisado por los verificadores independientes mediante una combinación de:

- Tecnología (*Machine Learning*).
- Denuncias de los usuarios.
- Revisión humana.
- Los propios *fact-checkers*.

A continuación, los verificadores eligen qué contenido revisar y calificar.

Finalmente, Facebook señala que actúa sobre el contenido calificado como falso por los *fact-checkers* degradándolo en el *News Feed*. Además, las páginas que compartan repetidamente contenido calificado como falso por

[36] Véase https://www.facebook.com/journalismproject/programs/third-party-fact-checking

[37] Véase https://transparency.fb.com/es-es/features/approach-to-ranking/types-of-content-we-demote/

los verificadores verán reducida la distribución de su página en la sección de noticias y se eliminará su capacidad de monetización y publicidad.

Desde la compañía se indica que se ha ampliado esta política para incluir también sanciones a las cuentas individuales. Asimismo, se puede reducir la distribución de otros contenidos sensacionalistas y de spam, como el *clickbait* y el *engagement bait*, que también pueden incluir desinformación.

c. Informar:

Facebook señala que quiere ayudar a prevenir la difusión de desinformación proporcionando contexto adicional y conectando a las personas directamente con información fiable para que puedan tomar decisiones informadas. Algunos ejemplos:

- Etiquetas de desinformación[38]. Se aplican etiquetas de advertencia y notificaciones en los contenidos verificados como falsos por los *fact-checkers*.
- Se añade un mensaje de advertencia a las personas que intentan compartir contenidos etiquetados como falsos para que se lo piensen dos veces. Cuando se coloca una pantalla de advertencia en una publicación, el 95% de las veces la gente no hace clic para verla[39].
- Más recientemente, Facebook ha empezado a mostrar mensajes en la sección de noticias para las personas a las que les ha gustado, han reaccionado o han comentado desinformación sobre la COVID-19 antes de que fuera eliminada, y a redirigirlos a la página web de la OMS donde se desmienten bulos. Se ha etiquetado y reducido la visibilidad de más de 167 millones de contenidos sobre la COVID-19 tras ser desmentidos por verificadores independientes.
- Además, la plataforma señala que informa a las personas antes de que sigan a una página que ha compartido repetidamente contenido que los *fact-checkers* han calificado como falso.
- Conecta a la gente con información precisa y autorizada:
    - Facebook lanzó el Centro de Información sobre la COVID-19 donde se incluyen actualizaciones en tiempo

[38] Véase https://www.facebook.com/journalismproject/programs/third-party-fact-checking/how-it-works

[39] Véase https://about.fb.com/news/2021/03/how-were-tackling-misinformation-across-our-apps/

real de las autoridades sanitarias nacionales (Ministerio de Sanidad en España) y de organizaciones mundiales como la OMS, así como artículos, vídeos y publicaciones útiles sobre el distanciamiento social y la prevención de la propagación de la COVID-19. La gente también puede seguir el Centro de Información sobre COVID-19 para recibir actualizaciones de las autoridades sanitarias directamente en su *News Feed*. Desde la plataforma se indica que se ha conectado a más de 2.000 millones de personas con recursos de las autoridades sanitarias a través del Centro de Información sobre COVID-19 y de ventanas emergentes educativas en Facebook e Instagram con más de 600 millones de personas que han hecho clic para obtener más información.

- Facebook e Instagram defienden que han lanzado productos, como el registro de votantes y los recordatorios del día de las elecciones, para conectar a las personas con información precisa sobre cuándo y cómo votar. En EE.UU., el Centro de Información sobre el Voto en Facebook e Instagram sirvió como un recurso para dar a los votantes estadounidenses las herramientas y la información que necesitaban para poder ejercer su voto en las urnas.

- Contexto adicional sobre el contenido que comparten las personas: la red social indica que ha introducido una nueva pantalla de notificación que permite a los usuarios saber si los artículos de noticias que van a compartir tienen más de 90 días de antigüedad.

- Alfabetización mediática y digital: También está invirtiendo en iniciativas de alfabetización mediática y digital para concienciar y ayudar a las personas a ser más críticas con la información que reciben. En España se lanzó GeneraZion, un programa educativo sobre seguridad en internet y alfabetización mediática para jóvenes que incluye formaciones en colegios y contenidos educativos interactivos en su plataforma digital[40].

[40] https://www.generazion.org/ En su segunda edición GeneraZion habría llegado a 15,000 estudiantes en formaciones directas en 200 colegios y a 75.000 más en la plataforma digital.

2. *Prevenir la injerencia/Operaciones de Influencia*

Desde Facebook se indica que una parte fundamental de la estrategia de la plataforma para prevenir las Operaciones de Influencia es trabajar con las autoridades gubernamentales, los cuerpos y fuerzas de seguridad, los expertos en seguridad, la sociedad civil y otras empresas tecnológicas para detener las amenazas emergentes y establecer una línea de comunicación directa para compartir conocimientos e identificar oportunidades de colaboración.

Como se ha mencionado en la sección de terminología, la no autenticidad y la coordinación son dos indicadores clave de las Operaciones de Influencia. Para combatir esta amenaza, Facebook defiende que ha desarrollado una política de comportamiento no auténtico que se dirige a los esfuerzos coordinados para manipular el debate público con un objetivo estratégico, donde las cuentas falsas son fundamentales para la operación[41]. Esto permite eliminar las redes de cuentas, páginas y grupos basándose en señales de comportamiento.

Al respecto, habría dos niveles de estas actividades:

1. El comportamiento inauténtico coordinado en el contexto de campañas nacionales no gubernamentales (CIB)[42].

2. El comportamiento inauténtico coordinado en nombre de un actor extranjero o gubernamental (FGI). En este sentido, Facebook señala que ha retirado más de 100 redes en todo el mundo por participar en comportamientos inauténticos coordinados (CIB) desde 2017.

Los actores que participan en Operaciones de Influencia no tienen por qué utilizar necesariamente la desinformación; la mayoría de los contenidos compartidos en campañas de Operaciones de Influencia no son probadamente falsos y, de hecho, serían un discurso político aceptable si fueran compartidos por actores auténticos. El verdadero problema es que los actores que están detrás de estas campañas utilizan comportamientos engañosos para ocultar su identidad para hacer que la organización o su actividad parezca digna de confianza o evadir los esfuerzos de aplicación de las normas.

---

[41] Véase https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/

[42] Véase https://about.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/

3. Aumentar la transparencia y el control de los usuarios

Facebook defiende que una mayor transparencia lleva a una mayor rendición de cuentas. Por este motivo, apuesta por la transparencia en la publicidad política y las páginas para que las personas puedan conocer quién está tratando de influir en ellos. Esto incluye:

- Anuncios políticos y temáticos: Los anuncios sobre temas sociales, elecciones o política incluyen avisos de "Pagado por" para mostrar quién está detrás del anuncio.
- Verificación de los anunciantes políticos: Para publicar un anuncio político o de temas sociales, los anunciantes deben pasar por un proceso de autorización, que puede incluir demostrar quiénes son y dónde viven[43].
- La biblioteca de anuncios ofrece una base de datos de anuncios de acceso público en la que se pueden realizar búsquedas y que permite a periodistas, reguladores, grupos de vigilancia, investigadores, académicos y personas en general exigir responsabilidades a los anunciantes[44]. Para ayudar investigar los anuncios, la biblioteca de anuncios ofrece:
    - una colección exhaustiva y con capacidad de búsqueda de todos los anuncios actualmente activos (políticos y no políticos) que se ejecutan en las aplicaciones y servicios de Facebook,
    - un archivo de anuncios políticos que permanecen en la biblioteca durante 7 años,
    - información agregada.
- Transparencia de la página: Facebook muestra información sobre las páginas como cuándo se creó, los cambios de nombre y la ubicación de los administradores de la página. También etiqueta a los medios de comunicación que creen que están total o parcialmente bajo el control editorial de su gobierno como medios controlados por el Estado[45].

---

[43] Véase https://www.facebook.com/business/help/issuesandpolitics

[44] Véase https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=ES&media_type=all

[45] Véase https://about.fb.com/news/2020/06/labeling-state-controlled-media/

- Información sobre la clasificación de las noticias: Los usuarios pueden hacer clic en la funcionalidad "¿Por qué estoy viendo esto?" y "¿Por qué estoy viendo este anuncio?" en las publicaciones y anuncios para entender por qué están viendo una noticia o contenido determinado, además de poder controlar lo que ven de sus amigos, páginas y grupos en la sección de noticias[46].

Además de la transparencia, desde Facebook se señala que es importante dar más control a las personas sobre los anuncios que ven, y por eso, en el caso de los anuncios políticos y de temas sociales, se habrían introducido controles para que la gente vea menos anuncios de este tipo en Facebook e Instagram.

A través de la herramienta Preferencias de Anuncios[47], los usuarios pueden desactivar todos los anuncios de temas sociales, electorales o políticos de candidatos, u otras organizaciones que tengan el aviso de exención de responsabilidad política "Pagado por".

---

[46] Véase https://about.fb.com/news/2019/03/why-am-i-seeing-this/ y https://www.facebook.com/help/562973647153813?helpref=faq_content

[47] Véase https://www.facebook.com/help/247395082112892?helpref=faq_content

RECOMENDACIONES Y PROPUESTAS DE ACTUACIÓN

Los miembros de este grupo de trabajo tienen el convencimiento de que la lucha contra la desinformación en los procesos electorales es una labor conjunta de la sociedad civil y los servidores públicos del Estado que pasa por la colaboración de periodistas, plataformas digitales, organizaciones de la sociedad civil, verificadores de datos, académicos, partidos políticos y poderes públicos.

Consideramos que esta lucha contra la desinformación debe descansar en una tríada compuesta por información, formación y prevención.

Esta lucha contra la desinformación debe descansar en una tríada compuesta por información, formación y prevención.

- La desinformación se combate con información y transparencia. El acceso a información veraz y diversa es uno de los pilares que sustentan las sociedades democráticas, y que deben asegurar las instituciones y administraciones públicas, porque permite a los ciudadanos formarse opinión sobre los asuntos políticos, participar en los debates públicos y votar con conocimiento y libertad. Los medios de comunicación, periodistas, partidos políticos e instituciones, pero también la sociedad civil y la ciudadanía deben defender y garantizar la transparencia, entendida como la materia prima para poder mejorar la calidad de nuestra democracia. Por este motivo, la libertad de expresión y el derecho a la información se consagran como derechos fundamentales en nuestra Constitución.
- La educación cívica es el antídoto contra la desinformación. En consecuencia, es necesario formar usuarios críticos con la información que reciben y consumen. La formación de los ciudadanos debe incluir un mínimo conocimiento de los procesos y sistemas electorales, derechos y deberes, garantías, etc. La competencia mediática y digital con capacidad crítica supone educar en lenguajes, tecnologías, procesos de interacción, procesos de producción y difusión, valores y estética.
- Ante las campañas de desinformación cada vez más sofisticadas son necesarias medidas de prevención a través de la cooperación público-privada para detectar, prevenir y combatir los ataques

durante las campañas electorales. Normas claras y procedimientos ágiles por parte de los poderes públicos, políticas de plataformas digitales con avanzadas metodologías de prevención contra las operaciones de influencia contra los ciudadanos y las instituciones; y un periodismo de calidad, riguroso y honesto.

Sobre esta tríada, este grupo realiza algunas propuestas o sugerencias a diferentes actores del proceso electoral, muchas de las cuales requerirán un desarrollo concreto posterior en caso de ser aceptadas.

Gráfico 9: Recomendaciones para dar respuesta a las campañas de desinformación en procesos electorales.
Elaborado por el DSN

Recomendaciones para la Administración Pública y el legislador

1. Se plantea la creación de un grupo de trabajo para el asesoramiento y seguimiento en la lucha contra la desinformación electoral que involucre a sociedad civil (academia, periodistas, verificadores, plataformas digitales, etc.), partidos políticos, Administración y JEC durante procesos electorales de carácter nacional, europeo, autonómico o local en España.

2. Reforma del artículo 50.1 Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG).

   Introducción de herramientas de alfabetización mediática y digital en las campañas institucionales del artículo 50.1 de la LOREG, bien incorporando en las ya existentes algún mensaje concreto en la materia, bien elaborando una campaña específica. Incluirá también información sobre el proceso electoral, el voto por correo, derechos de los ciudadanos, sistema de adjudicación de escaños, funciones de la Junta Electoral u otros organismos, etc.

   Ampliación de los canales de difusión de estas campañas, actualmente limitadas a los medios de comunicación de titularidad pública.

3. Modificar el artículo 69 de la LOREG. Suprimir la prohibición de publicar las encuestas electorales en los cinco días previos a la jornada de votación. La prohibición debería quedar limitada a las jornadas de reflexión y votación.

4. El art. 69 de la LOREG señala sobre la publicación de encuestas electorales: “1. Los realizadores de todo sondeo o encuesta deben, bajo su responsabilidad, acompañarla de las siguientes especificaciones, que asimismo debe incluir toda publicación de las mismas:

   - Denominación y domicilio del organismo o entidad, pública o privada o de la persona física que haya realizado el sondeo, así como de la que haya encargado su realización.
   - Características técnicas del sondeo, que incluyan necesariamente los siguientes extremos: sistema de muestreo, tamaño de la muestra, margen de error de la misma, nivel de representatividad, procedimiento de

selección de los encuestados y fecha de realización del trabajo de campo.

- Texto íntegro de las cuestiones planteadas y número de personas que no han contestado a cada una de ellas".

  La experiencia repetida de multitud de procesos electorales señala que esta información nunca se publica de manera completa. Por esta razón, se recomienda que el artículo 69 se actualice y recoja de manera adecuada la información que se ha de publicar y se haga cumplir su publicación.

En consonancia con la actualización de propuestas legislativas o normativas aprobadas sobre publicidad electoral de países como Canadá[48], EEUU[49] o Nueva Zelanda[50], así como de diferentes países de la Unión Europea (Furnémont y Kevin, 2020) y, sobre todo, ante la publicación, el 25 de noviembre de 2021, de la propuesta legislativa de la Comisión Europea sobre la transparencia en el contenido político patrocinado el cual debería guiar la actuación de España en este ámbito, se recomienda:

5. Modificar el Artículo 144 de la LOREG que hace referencia a "Delitos en materia de propaganda electoral" y señala que:

   "1. Serán castigados con la pena de prisión de tres meses a un año o la de multa de seis a veinticuatro meses quienes lleven a cabo alguno de los actos siguientes:

   a) Realizar actos de propaganda una vez finalizado el plazo de la campaña electoral".

   En los últimos años se ha comprobado que en ocasiones se han publicado anuncios políticos digitales durante la jornada de reflexión. Aunque no se constata una práctica generalizada, debería reforzarse el cumplimiento de la legislación electoral vigente o actualizar el artículo 144.

6. Establecer y desarrollar una nueva legislación sobre la publicidad electoral digital que incluya una definición exhaustiva, coherente con las normas de la Unión Europea, y uniforme de lo que ha de

[48] Véase: https://www.elections.ca/content.aspx?section=pol&dir=regifaq&document=index&lang=e

[49] Véase: https://www.congress.gov/bill/115th-congress/senate-bill/1989/text

[50] Véase: https://elections.nz/guidance-and-rules/for-voters/about-election-advertising/

considerarse como publicidad política digital. Esta nueva legislación actualizará, de acuerdo al desarrollo del nivel de vida, las infracciones y sanciones por incumplimiento de la ley.

7. La creación de un registro de publicidad electoral que aúne en un sitio web, gestionado por la Administración electoral competente, un repositorio, de acceso fácil y libre, que permita ver todos los anuncios de carácter político publicados o emitidos en los distintos medios y plataformas digitales, así como a las diferentes iniciativas de transparencia desarrolladas por parte de las plataformas, motores de búsqueda, aplicaciones o sitios web. Para la creación de este repositorio habrá que definir las plataformas en línea implicadas, si es necesario un mínimo de visitas mensuales para ser incluido en el registro, etc., en este ámbito. Se recomienda que las plataformas, motores de búsqueda, etc. ayuden a dar visibilidad a este repositorio como parte de su colaboración en las campañas de alfabetización digital sobre el funcionamiento del sistema electoral, fomentando la participación activa de la ciudadanía.
8. El registro electoral incluirá:
    - Una copia electrónica del anuncio que se muestra en la plataforma y el nombre de la persona que autorizó el anuncio.
    - Las iniciativas de transparencia sobre publicidad electoral incluidas en el registro de anuncios deberían extenderse al material electoral digital contratado en cualquier formato. Esta definición incluye, pero no se limita a textos, videos, carteles digitales, imágenes animadas o en movimiento, imágenes estáticas o grabaciones de audio.

La normativa establecerá un periodo de mantenimiento de cada anuncio en el registro. Este periodo no debe ser inferior a 4 años -o dos procesos electorales similares-.

Recomendaciones para las Juntas Electorales y Tribunal de Cuentas

Como se ha señalado, el contexto digital ha cambiado de forma significativa los procesos electorales. Desde esta perspectiva sería recomendable:

1. Reforma del artículo 19 de la LOREG. Dotar a la JEC de la posibilidad de que pueda recabar cuanta información y apoyo tecnológico precise de cualquier entidad, ya sea pública o privada. A tal efecto, los requerimientos de la Junta en esta materia deberán ser atendidos con la inmediatez que exigen los plazos fugaces en los que se desarrolla todo proceso electoral, de manera que sea posible responder eficazmente a las posibles amenazas híbridas, campañas de desinformación u otros escenarios que puedan distorsionar la transparencia y objetividad con que deben desarrollarse unas elecciones.

2. En las semanas iniciales de cada proceso electoral deben ponerse en marcha campañas informativas de las funciones de la Administración Electoral, a fin de resolver las dudas más comunes de los ciudadanos y los medios de comunicación acerca de los procedimientos y competencias de las diferentes juntas electorales en materia de constitución de mesas, voto por correo, voto de personas con discapacidad, impugnaciones, recursos etc.

3. Promover una actitud más proactiva por parte de JEC en materia de comunicación pública, en coordinación con las Juntas Provinciales, mejorando también la accesibilidad de su página web, así como mediante la creación de perfiles institucionales en las principales redes sociales.

4. Sin perjuicio de las facultades de supervisión que puedan corresponder a la JEC, se deben concentrar en el Tribunal de Cuentas las facultades de control jurisdiccional y contable de las normas relativas a las cuentas y gastos electorales de las candidaturas, así como ampliar los mecanismos de transparencia y rendición de cuentas exigidos a las diferentes candidaturas, especificando y publicando en formato abierto los gastos realizados en publicidad electoral.

Recomendaciones para los partidos políticos

1. Recomendación de reforzar la seguridad digital en línea con lo expuesto en el apartado de Recomendaciones sobre ciberseguridad destinadas a combatir la desinformación.
2. Proponer y animar a los partidos políticos a que acuerden un código de conducta que ayude a las partes a unirse contra la desinformación o al menos denunciar a quienes la utilizan[51]. Un foro adecuado para alcanzar este consenso es la Ponencia sobre Desinformación de la Comisión Mixta de Seguridad Nacional. Se trataría de un compromiso entre las partes y de cara al electorado.
3. Identificar debidamente toda publicidad electoral en cualquier medio o plataforma tecnológica, así como cualquier recurso pagado para persuadir al electorado como, por ejemplo, la contratación de personas influyentes (*influencers*).
4. Las entidades políticas que contraten un servicio de publicidad política digital deberán proporcionar toda la información necesaria y veraz para que la plataforma cumpla con las disposiciones del registro propuesto, así como el compromiso de cumplir la normativa electoral como, por ejemplo, en lo referido a la jornada de reflexión.
5. Se recomienda a los partidos políticos que, en un ejercicio de transparencia, informen sobre las organizaciones o empresas contratadas para la creación, producción y gestión de la publicidad digital electoral.

[51] Un código de ejemplo puede ser el propuesto por IDEA Internacional para los Países Bajos. Cfr. https://www.idea.int/sites/default/files/news/news-pdfs/Dutch-Code-of-Conduct-transparency-online-political-advertisements-EN.pdf

Recomendaciones para las plataformas sociales

1. Se recomienda la distinción de la publicidad electoral frente al resto de anuncios publicitarios en cualquier tipo de plataforma digital.
2. Se recomienda la obligación de que las plataformas tecnológicas publiquen, en línea con las recomendaciones de la Comisión Europea respecto al actual proceso de actualización del Código de la UE sobre desinformación, al menos:
    - Un informe de transparencia específico sobre nuestro país anexo a los informes de transparencia del Código de la UE sobre desinformación.
    - Un informe sobre las operaciones de información, posibles operaciones de influencia extranjera, etc.
    - Las políticas de actualización de normas, etc.
3. Se recomienda la necesidad de identificar mediante una etiqueta cualquier cuenta automatizada (*bot*).
4. Se recomienda que las plataformas sociales establezcan equipos específicos durante las elecciones generales en España para combatir la desinformación[52].
5. Se recomienda que las plataformas digitales impulsen la alfabetización digital sobre el funcionamiento del sistema electoral, fomentando la participación activa de la ciudadanía.
6. Deberán colaborar aportando sus iniciativas de transparencia en el registro de publicidad electoral señalado en el apartado de Recomendaciones para la Administración Pública y el legislador.
7. Se recomienda que las plataformas y redes sociales desarrollen una herramienta de Preferencias de Anuncios, donde los usuarios puedan desactivar todos los anuncios de temas electorales o políticos de candidatos, partidos u otras organizaciones que tengan el aviso de exención de responsabilidad.

[52] Véase, por ejemplo, https://about.fb.com/news/2021/10/protecting-us-2020-elections-inauguration-day/ y https://help.twitter.com/es/using-twitter/us-elections

Recomendaciones para los medios de comunicación y verificadores

Los medios de comunicación y los periodistas son actores principales del proceso informativo y, por tanto, están llamados a tener protagonismo en el combate contra la desinformación.

1. Se recomienda un mayor esfuerzo por la transparencia y buen gobierno tanto de los medios de comunicación como de los verificadores. Se entiende por transparencia voluntaria el esfuerzo por difundir y publicar la información relevante de la organización, haciéndola visible y accesible a todos los grupos de interés de manera íntegra y actualizada. La transparencia de los medios y verificadores redunda en beneficio de su credibilidad e independencia. En consecuencia, se anima a cada medio a publicar la información relevante sobre su Propiedad, el Gobierno, la Información económica, así como la creación y divulgación de contenidos editoriales.
2. En este sentido, se recomienda reforzar las medidas de transparencia y rendición de cuentas de medios estatales extranjeros que operan en nuestro país a través de canales de TDT, por suscripción o satélite y que emitan en algunas de las lenguas cooficiales del Estado. Entre estas medidas, además de las especificadas en el punto anterior, podrían señalarse a título de ejemplo: advertir sobre la financiación estatal de estas televisiones en informaciones relacionadas con nuestro país durante procesos electorales, asegurar los mecanismos para ejercer el derecho de réplica y rectificación, etc.
3. Colaborar de forma activa en las campañas de alfabetización mediática y digital que mejoren las competencias de los ciudadanos en el uso de la información en procesos electorales[53].

[53] En el capítulo 3 se sintetizan algunas actividades de alfabetización mediática que realizan periodistas y verificadores. Sería conveniente ampliarlas y concretarlas para procesos electorales.

Recomendaciones sobre ciberseguridad destinadas a combatir la desinformación

La gestión de las amenazas híbridas, vulnerabilidades en temas de ciberseguridad y las consecuencias que se presentan en el contexto actual requiere de una labor coordinada entre los distintos actores implicados en la lucha contra la desinformación[54].

Este grupo de expertos recomienda que las autoridades competentes elaboren una guía de ciberseguridad[55] para partidos políticos[56] -independientemente del ámbito del proceso electoral al que concurran: europeo, estatal, autonómico o local- que contemple, como mínimo, las siguientes cuestiones:

- Protocolo de seguridad en caso de pérdida/robo de dispositivos electrónicos y teléfonos móviles que puedan comprometer información relativa a cualquier partido político.
- Protocolos de seguridad en la gestión de servidores en la nube y acceso a redes.
- Protocolos de seguridad de claves y contraseñas vinculados a cualquier formación política.
- Protocolos de seguridad en la gestión de redes sociales.
- Protocolo de seguridad en la gestión y protección de datos.
- Protocolos de capacitación de personal en cuestiones de ciberseguridad: *phishing*, *hacking*…

[54] Véase: https://www.belfercenter.org/publication/cybersecurity-campaign-playbook

[55] El Centro Criptológico Nacional (CCN) ha manifestado su disposición a asesorar en la redacción de esta guía con el protocolo de seguridad para los partidos políticos.

[56] Las recomendaciones en este apartado se limitan a la guía para partidos políticos, porque existen herramientas de garantía de la seguridad en la difusión de resultados provisionales. Así, la Orden INT/424/2019, de 10 de abril, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio del Interior y las directrices generales en materia de seguridad de la información para la difusión de resultados provisionales en procesos electorales, tiene entre sus objetivos fortalecer la capacidad de identificación, detección, prevención, contención y adecuada gestión ante posibles ciberamenazas en el ámbito de los procesos electorales, coordinando actuaciones a través de la creación del Subcomité de Seguridad de la Información en Procesos electorales, adscrito al Comité Superior para la Seguridad de la Información.

- Protocolos que establezcan una definición de información sensible y reglas para su uso, incluido el equipo de operaciones y las distintas funciones de cada uno de sus miembros.
- Protocolos que establezcan como actuar en caso de que algún miembro de un partido político reciba algún tipo de información o mensaje sospechoso.
- Protocolo de respuesta legal en caso de ciberataque.

Recomendaciones sobre coordinación de la sociedad civil

1. Creación de una base de datos o repositorio de acceso público sobre contenidos desinformativos de índole electoral[57].
2. Coordinar y activar proyectos colaborativos de verificación durante procesos electorales[58]. Se plantea explorar y consolidar iniciativas que integren a academia, verificadores, organizaciones de la sociedad civil, agencias de noticias, medios digitales, periódicos, radios, televisiones o medios especializados para verificar el discurso público y político en campaña electoral, y que cuenten con la colaboración de las plataformas sociales.
3. Desarrollar mecanismos de alfabetización sobre las campañas electorales. La educación cívica es el antídoto contra la desinformación. Por ello, el grupo de trabajo para la monitorización electoral, que se propone crear, asesorará en la elaboración de contenidos de alfabetización dirigidos a los electores para que les ayuden a identificar y verificar contenidos falsos en internet. Esta iniciativa irá dirigida a toda la población y podrá ser emitida en espacios similares a los que actualmente se reserva a la propaganda electoral en los principales medios de comunicación social y en las principales plataformas digitales.
4. Proponer el uso de *serious games*[59] para impulsar la alfabetización en materia electoral y la identificación de desinformación de modo que se pueda alcanzar a colectivos que no participan aún de los procesos electorales (adolescentes) y que utilizan un lenguaje y unas narrativas audiovisuales diferentes.

---

[57] Podría encargarse de esta base de datos el proyecto Iberifier –Iberian Digital Media Research and Fact-Checking Hub–, que investiga los cibermedios y monitoriza las amenazas de la desinformación en España y Portugal. Conforma el hub regional de la península ibérica, uno de los ocho que formarán parte del European Digital Media Observatory de la Unión Europea. https://www.researchgate.net/project/IBERIFIER-Iberian-Digital-Media-Research-and-Fact-Checking-Hub

[58] Como ya ocurrió en 2019 en España con la iniciativa Comprobado. https://maldita.es/maldito-dato/20190411/comprobado-16-medios-unidos-para-luchar-contra-la-desinformacion-y-la-mentira-politica-en-elecciones/

[59] Los *serious games* son juegos diseñados con un propósito formativo más que para fines de entretenimiento

CONCLUSIONES

La Comisión de la UE ha señalado que “la democracia no puede darse por sentada. Necesita ser cuidada y protegida de forma activa” y que “El mantenimiento de la democracia exige una actuación más decidida para proteger los procesos electorales, conservar el debate abierto democrático y actualizar las salvaguardias a la luz de las nuevas realidades digitales” (Plan de Acción para la Democracia Europea de diciembre de 2020).

La lucha contra la desinformación en procesos electorales exige el trabajo coordinado de todos y requiere involucrar de manera principal a la sociedad civil a través de tres pilares esenciales como son la transparencia, la educación y la prevención.

La lucha contra la desinformación en procesos electorales exige el trabajo coordinado de todos y requiere involucrar a la sociedad civil.

Las herramientas para conseguirlo son diversas y en el presente trabajo se ha incluido un nutrido catálogo. Se trata de medidas que van más allá del momento en el que se convoca un proceso electoral y que se extienden en el tiempo con la finalidad de construir un entorno en el que la desinformación tenga un escaso margen de maniobra.

En ese sentido, el Grupo ha hecho especial hincapié en la necesidad de reforzar la información institucional y de ofrecer la mayor la transparencia posible en todos los aspectos relacionados con el proceso electoral.

Sin embargo, la evolución de la tecnología y de nuestra propia sociedad exige una revisión constante de la materia. Por ello, quizá, una de las conclusiones más relevantes de los trabajos realizados sea la necesidad de disponer de un foro estable de contacto, comunicación y trabajo que permita enfrentarse a cada proceso electoral. De este modo, el grupo de trabajo ha decidido formalizar su carácter permanente, y sus integrantes se han comprometido a volver a encontrarse de manera recurrente para analizar si es necesario adoptar nuevas miradas y nuevas medidas en futuros procesos electorales y, por qué no, para evaluar la implementación de las recomendaciones y propuestas realizadas.

REFERENCIAS BIBLIOGRÁFICAS

Alaphilippe, A., Gizikis, A., Hanot, C., Y Bontcheva, K. (2019). *Automated tackling of disinformation*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf

Allcott, H. y Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election, *Journal Of Economic Perspectives*, 31(2), 211-236. https://doi.org/10.1257/jep.31.2.211

BBC News Mundo. (17 de febrero, 2021). Elecciones en Ecuador: la crisis desatada por el recuento de votos en las presidenciales (y qué consecuencias puede tener). *BBC*. https://www.bbc.com/mundo/noticias-america-latina-56093023

Bennett, W.L. y Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), 122-139. https://doi.org/10.1177/0267323118760317

Bradshaw, S. y Howard, P.N. (2019). *The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation*. Oxford Internet Institute. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Cadwalladr, C. y Graham-Harrison, E. (17 marzo, 2018). How Cambridge Analytics turned Facebook 'likes' into a lucrative political tool. *The Guardian*. https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm

Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías. (2018). *A multi-dimensional approach to disinformation: report of the independent High level Group on fake news and online disinformation*. Publications Office. https://data.europa.eu/doi/10.2759/739290

Comisión Europea. (2018b). *Garantizar unas elecciones europeas libres y justas Contribución de la Comisión Europea a la reunión de los dirigentes*

en Salzburgo los días 19 y 20 de septiembre de 2018, (COM(2018) 637 final). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX-:52018DC0637&from=EN

Comisión Europea. (2018c). *Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

Comisión Europea. (2018d). *Plan de Acción contra la Desinformación* (JOIN(2018) 36 final). https://data.consilium.europa.eu/doc/document/ST-15431-2018-INIT/es/pdf

Comisión Europea. (2021). *Orientaciones de la Comisión Europea sobre el refuerzo del Código de Buenas Prácticas en materia de Desinformación* (COM(2021) 262 final). https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52021DC0262

Furnémont, J.-F. y Kevin, D. (2020). *Regulation of political advertising: A comparative study with reflections on the situation in South-East Europe*. Consejo de Europa. https://rm.coe.int/study-on-political-advertising-eng-final/1680a0c6e0

De Keersmaecker, J. y Roets, A. (2017). Fake news: Incorrect, but hard to correct. The role of cognitive ability on the impact of false information on social impressions. *Intelligence*, 65, 107-110. https://doi.org/10.1016/j.intell.2017.10.005

Dickey, L., (2019). Confronting the Challenge of Online Disinformation in Taiwan. En Y. Tatsumi, P. Kennedy y J. Li (Eds.), *Taiwan Security Brief: Disinformation, Cybersecurity, and Energy Challenges* (11-22). Washington, DC: Stimson Center.

Ferrara, E. (2020). Bots, elections, and social media: a brief overview. En K. Shu, S. Wang, D. Lee, H. Liu (Eds.), *Disinformation, Misinformation, and Fake News in Social Media* (95-114). Lecture Notes in Social Networks. Springer Cham.

Guess, A., Nyhan, B., y Reifler, J. (2018). Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 US presidential campaign. *European Research Council*, 9.

Hacquebord, F. (2017). Two Years of Pawn Storm Examining an Increasingly Relevant Threat. *TrendLabs Research Paper*. https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf

Hall Jamieson, K. (2018). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President. What we don't, can't, and do know*, Oxford University Press, Oxford. https://dx.doi.org/10.1093/oso/9780190058838.001.0001

Krzyżanowski, M. (2019). Brexit and the imaginary of 'crisis': a discourse-conceptual analysis of European news media. *Critical Discourse Studies*, 16(4), 465-490. https://doi.org/10.1080/17405904.2019.1592001

Magallón Rosa, R. (2019). Verificado México 2018: Desinformación y fact-checking en campaña electoral. *Revista de comunicación*, 18(1), 234-258. https://revistadecomunicacion.com/article/view/1034

Martínez, M. (30 de mayo, 2018). Mexico election: Concerns about election bots, trolls and fakes. *BBC*. https://www.bbc.com/news/blogs-trending-44252995

Newman, N., Fletcher, R., Kalogeropoulos, A., Kalogeropoulos, A., Levy, D., y Nielsen, R.K. (2018). *Reuters Institute Digital News Report 2018*. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/digital-news-report-2018.pdf

Norris, P., Frank, R., y Martínez i Coma, F. (2015) *Contentious Elections: From Ballots to Barricades*, Routledge, London-New York.

Paniagua, F., Seoane, F., y Magallón-Rosa, R. (2020). Anatomía del bulo electoral: la desinformación política durante la campaña del 28-A en España. *Revista CIDOB d'Afers Internacionals*, 124, 123-145. https://doi.org/10.24241/rcai.2020.124.1.123

Parlamento Europeo. (2020). *Resolución sobre el balance de las elecciones europeas* (2020/2088(INI)). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0327_ES.html

Puig, S. (2017). Desinforma, que algo queda: el fenómeno de las fake news en el siglo XXI. *Agenda Pública*. http://agendapublica.elperiodico.com/desinforma-algo-queda-fenomeno-las-fake-news-siglo-xxi/

Rubio Núñez, R. (2018). Los efectos de la posverdad en la democracia. *Revista De Derecho Político*, 1(103), 191–228. https://doi.org/10.5944/rdp.103.2018.23201

Silverman, C. y Alexander, L. (4 de noviembre, 2016). How Teens in The Balkans Are Duping Trump Supporters with Fake News. *Buzzfeednews*. ht-

tps://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo

Stanford Internet Observatory (21 de enero, 2020). Taiwan Election: Disinformation as a Partisan Issue, *Stanford University, Freeman Spogli Institute for International Studies*, Recuperado el 9 de septiembre de 2021 de https://fsi.stanford.edu/news/taiwan-disinformation-partisan-issue.

Subramanian, S. (15 de febrero, 2017). Inside the Macedonian fake-news complex. *Wired*. https://www.wired.com/2017/02/veles-macedonia-fake-news/

Torres Soriano, M. R. (2017). Hackeando la democracia: operaciones de influencia en el ciberespacio. *bie3: Boletín IEEE*, (6): 826-839. https://www.ieee.es/contenido/noticias/2017/06/DIEEEO66-2017.html

Vosoughi, S., Roy, D., y Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380): 1146-1151. http://doi.org/gc3jt6

Wardle, C. (14 de marzo, 2017). Noticias falsas. Es complicado. *First Draft News*. https://firstdraftnews.org/articles/noticias-falsas-es-complicado/

ANEXO 1: Sobre las desinformaciones más viralizadas en internet en los últimos procesos electorales en España

Fecha de detección	Afirmación	Resultado de la verificación	Explicación	Visto en	Enlace al contenido	Enlace al fact-check	Convocatoria electoral	Tipo de desinformación	Formato	Motivación
Recurrente desde finales de 2018	Pablo Casado ha dicho "cada cual cobra lo que se merece, los que cobran el salario mínimo, es porque su trabajo es mínimo y no merecen más"	No hay pruebas	Cita falsa	WhatsApp, Facebook	https://maldita.es/app/upl	https://maldita.es/malditobulo/n	Generales noviembre de 2019	Contenido fabricado		
19/10/2019	Manipulación descarada del censo electoral: 200.000 personas inmigrantes ilegales	Bulo	Los inmigrantes no pueden votar. Esos 200.000 son nuevos votantes que han alcanzado la mayoría de edad	WhatsApp, Twitter	https://twitter.com/jm_cla	https://maldita.es/malditobulo/2	Generales noviembre de 2019	Contenido engañoso	Video	desacreditar al proceso electoral
20/10/2019	Vídeo de Albert Rivera hablando drogado	Bulo	Es un vídeo ralentizado	WhatsApp, Twitter	https://twitter.com/photoc	https://maldita.es/malditobulo/2	Generales noviembre de 2019	Contenido manipulado	Video	desacreditar a un candidato/partido
30/10/2019	Santiago Abascal sale en los Papeles de Bárcenas	Bulo	Es su padre	WhatsApp, Twitter, Facebook	https://maldita.es/upload	https://maldita.es/malditobulo/2	Generales noviembre de 2019	Contexto falso	Imagen	desacreditar a un candidato/partido
06/11/2019	Pedro Sánchez dicta un DECRETO DE CENSURA EN REDES a 2 dias de las elecciones	Bulo	El decreto no afecta al contenido de las redes sociales y las interrupciones de servicio ya estaban contempladas por la ley	YouTube, WhatsApp, Instagram, Twitter	https://www.youtube.com	https://maldita.es/malditobulo/2	Generales noviembre de 2019	Contenido engañoso,	Video, imagen	desacreditar a un candidato/partido, desacreditar al proceso electoral
06/11/2019	Propaganda electoral con las papeletas con la fecha cambiada al "19 de noviembre"	Bulo	Las papeletas son válidas y el "19" alude al año	Twitter, WhatsApp	https://maldita.es/app/upl	https://maldita.es/malditobulo/2	Generales noviembre de 2019	Contenido engañoso, contexto falso	Imagen	desacreditar al proceso electoral
08/11/2019	Personas que no estan en el padrón pero si en el censo electoral pucherazo pedro sanchez huelva	No hay pruebas	El Ayuntamiento dice que el caso del vídeo fue un error de impresión y la Junta Electoral niega haber recibido quejas	Twitter, Facebook, WhatsApp, YouTube	https://www.youtube.com	https://maldita.es/malditobulo/2	Generales noviembre de 2019	Contenido engañoso	Video	desacreditar a un candidato/partido, desacreditar al proceso electoral
09/11/2019	El PP ha violado la ley de Protección de Datos haciendo uso de una "empresa americana sufragada por Soros"	No hay pruebas	La empresa Iberinfo no es americana y no hay pruebas de que esté financiada por el empresario George Soros	Twitter, WhatsApp	https://maldita.es/maldito	https://maldita.es/malditobulo/n	Generales noviembre de 2019	Contenido engañoso	Texto	desacreditar a un candidato/partido
10/11/2019	Los votantes de la derecha deben meter tres papeletas (PP, Cs y Vox) en el sobre para que la derecha no pierda votos	Bulo	Ese voto sería nulo	Twitter, WhatsApp	https://twitter.com/Valenc	https://www.publico.es/politica/	Generales noviembre de 2019	Contenido engañoso	Tuit, Texto	desacreditar a un candidato/partido, desacreditar al proceso electoral
10/11/2019	El líder del PP, Pablo Casado, sujeta una bandera franquista en una fotografía	Bulo	Es un fotomontaje	Twitter	https://www.publico.es/po	https://www.publico.es/politica/	Generales noviembre de 2019	Contenido manipulado	Imagen	desacreditar a un candidato/partido
10/11/2019	Sánchez critica a la JEC por abrirle un expediente por dar una entrevista a La Sexta en La Moncloa	Bulo	Es una cuenta paródica	Twitter	https://twitter.com/sanche	https://www.publico.es/politica/	Generales noviembre de 2019	Sátira / Parodia	Tuit	desacreditar a un candidato/partido
05/02/2021	Comunicado del Govern en el que aclaran que en las elecciones de Cataluña sólo se puede votar una vez	Bulo	No encontramos que este comunicado haya sido publicado por una fuente oficial	WhatsApp, Twitter	https://maldita.es/upload	https://maldita.es/malditobulo/2	Cataluña febrero de 2021	Contenido fabricado	Imagen,Tuit	desacreditar a un candidato/partido, desacreditar al proceso electoral
12/02/2021	Illa da positivo por coronavirus en el Hospital Quirón de Barcelona	Bulo	El hospital afirma que el documento está "trucado" y niega que exista ningún análisis con ese nombre	WhatsApp, Twitter	https://maldita.es/upload	https://maldita.es/malditobulo/2	Cataluña febrero de 2021	Contenido fabricado	Imagen,Tuit	desacreditar a un candidato/partido
07/04/2021	La UE exige a Sánchez elecciones anticipadas antes de soltar un solo duro	Bulo	La Comisión Europea y el Parlamento Europeo aseguran que el contenido es "completamente falso". No hubo elecciones, pero sí se firmaron los fondos	Facebook, WhatsApp	https://maldita.es/upload	https://maldita.es/malditobulo/2	C. de Madrid mayo de 2021	Contenido fabricado	Imagen, Texto, Audio	desacreditar a un candidato/partido
09/04/2021	Alberto Garzón dice que las mujeres son mas propensas a quedarse embarazadas que los hombres	Bulo	No hay rastro de estas declaraciones por parte del ministro de Consumo y el autor del montaje afirma que "es coña".	Twitter, Facebook, WhatsApp	https://twitter.com/Carluc	https://maldita.es/malditobulo/2	C. de Madrid mayo de 2021	Contenido fabricado	Imagen, Texto	desacreditar a un candidato/partido
19/04/2021	Un camión con el logo de Vox y otro con el de Podemos queda atascado bajo un puente en Madrid	Bulo	La imagen ha sido manipulada para incluir el logo de ambos partidos	Twitter, Facebook	https://verifica.efe.com/la	https://verifica.efe.com/la-foto-d	C. de Madrid mayo de 2021	Contenido manipulado	Imagen	desacreditar a un candidato/partido
21/04/2021	Están enviando papeletas falsificadas del PP en las que han incluido a Toni Cantó y que serán nulas si se utilizan	Bulo	No hay fotos ni ninguna otra evidencia, el PP lo niega	WhatsApp	https://maldita.es/upload	https://maldita.es/malditobulo/2	C. de Madrid mayo de 2021	Contenido fabricado	Imagen, Texto	desacreditar a un candidato/partido, desacreditar al proceso electoral

Fecha de detección	Afirmación	Resultado de la verificación	Explicación	Visto en	Enlace al contenido	Enlace al fact-check	Convocatoria electoral	Tipo de desinformación	Formato	Motivación
28/04/2021	**Correos manipula el voto por correo. La prueba es que imprime tiques con el concepto "votos emitidos" a clientes que no han depositado su voto**	No hay pruebas	No hay pruebas que demuestren la manipulación. Es un error informático a la hora de expedir el comprobante de caja	WhatsApp, Twitter, Facebook	https://verifica.efe.com/la	https://verifica.efe.com/las-fals	C. de Madrid mayo de 2021	Contenido engañoso	Texto	desacreditar a un candidato/partido, desacreditar el proceso electoral
28/04/2021	**Hay un millón de votos por correo desaparecidos**	Bulo	Es un cálculo tramposo que ignora a los votantes que forman parte del Censo Electoral de Residentes Ausentes (CERA)	WhatsApp, Twitter, Facebook	https://verifica.efe.com/la	https://verifica.efe.com/las-fals	C. de Madrid mayo de 2021	Contenido engañoso	Texto	desacreditar el proceso electoral
28/04/2021	**Indra interfiere en el recuento electoral para alterar el escrutinio**	Bulo	Indra automatiza el envío de los datos, pero el recuento se hace en las mesas de votación	WhatsApp, Twitter, Facebook	https://verifica.efe.com/la	https://verifica.efe.com/las-fals	C. de Madrid mayo de 2021	Contenido engañoso	Texto	desacreditar el proceso electoral
28/04/2021	**Correos publica el porcentaje de votos emitidos**	Bulo	Es una publicación "irónica". Correos no ha hecho públicos esos datos	Twitter, Facebook	https://archive.is/HEI15	https://verifica.efe.com/las-fals	C. de Madrid mayo de 2021	Parodia	Fotografía	desacreditar el proceso electoral
01/05/2021	**Isabel Díaz Ayuso ha dicho que "en Ávila, vas por la calle y te encuentras aguas fecales o basura en los suelos" y que eso en Madrid "no pasa" porque hay "un gran sistema de alcantarillado**	Bulo	El usuario en Twitter que se hacía pasar por el medio Electomanía ha reconocido que Díaz Ayuso no ha pronunciado esa frase y que se trataba de una broma.	Twitter	https://twitter.com/louiew	https://maldita.es/malditobulo/2	C. de Madrid mayo de 2021	Contenido impostor	Texto	desacreditar a un candidato/partido
03/05/2021	**El nombre de Vox sale de la Alemania Nazi**	No hay pruebas	Ya en 2017, Vox subió un vídeo de Santiago Abascal explicando que "esta alternativa política se llama Vox desde el principio, 'vox', en latín", ya que, según él, "había muchos españoles que se habían quedado políticamente huérfanos, que se habían quedado sin voz,"	WhatsApp, Twitter, Facebook	https://maldita.es/upload	https://maldita.es/malditobulo/2	C. de Madrid mayo de 2021	Contenido fabricado	Imagen, texto	desacreditar a un candidato/partido
04/05/2021	**Las cartas con balas dirigidas a Iglesias y Grande Marlaska, fueron enviadas por el jefe de seguridad de Podemos**	Bulo	Es una imagen manipulada que buscar asemejarse a un titular del diario El País	WhatsApp	https://maldita.es/upload	https://maldita.es/malditobulo/2	C. de Madrid mayo de 2021	Contenido fabricado	Imagen	desacreditar a un candidato/partido

CAPÍTULO 5

PRINCIPIOS PARA UNA ESTRATEGIA CONTRA LA DESINFORMACIÓN

Coordinador sociedad civil:

Félix Arteaga Martín (Real Instituto Elcano)

Coordinador institucionall:

Departamento de Seguridad Nacional

Autores y colaboradores:

Emilio Andreu Jiménez (Asociación de Periodista de Defensa)

Miguel Ángel Aguilar (Asociación de Periodistas Europeos)

Alejandro Perales Albert (Asociación de Usuarios de la Comunicación)

José Domingo Gómez Castallo (Asociación para la Autorregulación de la Comunicación Comercial)

Elena Martínez Marín (Asociación para la Autorregulación de la Comunicación Comercial)

Desirée García Pruñonosa (EFE verifica)

José Ignacio Torreblanca Payá (European Council on Foreign Relations)

Javier Castro-Villacañas (Federación de Asociaciones de Radio y Televisión de España)

Ana Abade Gil (Google)

Manuel Ricardo Torres Soriano (Instituto de Seguridad y Cultura)

Carlos Hernández-Echevarría (Maldita.es)

Guillermo Serrano Peña (Meta)

Lorenzo Cotino Hueso (Plataforma en Defensa de la Libertad de Información)

Beatriz Correyero Ruiz (Red de Colegios de Periodistas)

María de Reparaz de la Serna (Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales)

Camino Rojo Torres (Twitter)

Raúl Magallón Rosa (Universidad Carlos III de Madrid)

Raquel Vinader Segura (Universidad Rey Juan Carlos)

María del Mar López Gil (Accenture)

INTRODUCCIÓN

Este documento tiene como finalidad proponer las bases para la elaboración de una Estrategia nacional de lucha contra las campañas de desinformación (en adelante, la Estrategia). El Grupo de Trabajo recibió este mandato como colofón a las tareas específicas que se encargaron a los otros grupos de expertos (Capítulos 1 a 4). A diferencia de otras estrategias, donde la valoración pública de las mismas se conoce tras su aprobación, en esta ocasión el Departamento de Seguridad Nacional ha preferido invertir el procedimiento y recabar antes las opiniones de la sociedad civil y el sector privado. Para ello se articuló un grupo en el que han participado representantes de los medios de comunicación y sus asociaciones profesionales, plataformas digitales, agencias de verificación, universidades y *think tanks* familiarizados con el fenómeno de la desinformación.

A diferencia de otras estrategias, donde la valoración pública de las mismas se conoce tras su aprobación, en esta ocasión se ha invertido el procedimiento y se ha recabado antes las opiniones de la sociedad civil y el sector privado.

En este marco, este Grupo de Trabajo ha integrado las reflexiones y conclusiones propias y de los otros grupos a propósito de los elementos que componen la estructura básica de una estrategia. En primer lugar, delimitar el concepto de desinformación y conocer su impacto en la seguridad internacional, los efectos que causan y las medidas de seguridad adoptadas por otros actores nacionales y multilaterales. En segundo lugar, determinar la importancia de las campañas de desinformación para la seguridad nacional y los límites que se deben fijar a las acciones de respuesta. Finalmente, identificar los posibles objetivos de la Estrategia, así como el sistema y procedimientos de funcionamientos desde el punto de vista de la sociedad civil.

Se espera que las conclusiones y recomendaciones de este capítulo desde una perspectiva civil ayuden a los responsables gubernamentales a elaborar una Estrategia con un enfoque de construcción social, integrando las visiones pública y privada del problema de la desinformación.

Se espera que las conclusiones y recomendaciones ayuden a los responsables gubernamentales a elaborar una Estrategia con un enfoque de construcción social, integrando las visiones pública y privada del problema de la desinformación.

Asimismo, cualquier iniciativa nacional deberá estar coordinada con los planes existentes a nivel europeo, como el Plan de Acción contra la Desinformación y el Plan de Acción para la Democracia Europea, así como con los trabajos elaborados por el Servicio Europeo de Acción Exterior relativo a las campañas de desinformación y sobre la manipulación e injerencia en la información extranjera.

LA DESINFORMACIÓN COMO CONCEPTO

La conceptualización de la desinformación es una tarea importante y, delimitarla, especialmente si afecta a derechos y libertades fundamentales, obliga a que las estrategias nacionales manejen conceptos concretos y restrictivos[1]. Como concepto, este Grupo utiliza el recomendado en el Capítulo 1 que se corresponde con el adoptado por la Comisión Europea (2018a) y que es una referencia europea e internacional.

Se considera desinformación a "la información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para inducir a error deliberadamente a la población, y que puede causar un perjuicio público". Según el citado Capítulo 1, se debe diferenciar desinformación de noticias falsas (*fake news*) porque estas son un concepto ambiguo, difícil de acotar y sin consenso académico (Salaverría-Aliaga, 2021; Rodríguez Pérez, 2019; Nielsen y Graves, 2017; Weedon et al., 2017; Wardle y Derakhshan, 2017)[2]. Si es falso, no es noticia; y si es noticia, y por tanto ha habido verificación de contenidos, no es falso (Mayoral et al., 2019)[3].

Para la Comisión Europea, la desinformación requiere también la intencionalidad y el encubrimiento de sus autores, actuaciones y objetivos. Sin embargo, no incluye errores involuntarios, sátira y parodia, u opiniones claramente identificadas como partidistas (Comisión Europea, 2018c). Además, la desinformación es diferente de la información con contenidos falsos o engañosos compartida sin intención de perjudicar, independientemente de los daños que pueda causar (información engañosa, también referida como *misinformation*).

[1] Ee el Capítulo 2 se resalta el contraste entre la concreción y restricción de los conceptos normativos en los países democráticos y la amplitud de estos en los países no democráticos.

[2] A pesar de que el concepto acuñado por la UE sitúa en igualdad la intención lucrativa y la de inducir a error a la opinión pública, este Grupo se considera que este último elemento es mucho más relevante que el primero para su consideración como problema de seguridad nacional.

[3] Una noticia da cuenta de un acontecimiento de la realidad. Es falsa cuando no se compadece con ella. No siempre es posible saber si una noticia es verdadera o falsa, pero se le exige comprobación de los hechos y que no tenga voluntad de inducir a error. Un rumor no es noticia porque se trata de una información no verificada o verificable, sea verdadera o falsa.

Por otro lado, en el Capítulo 1 también se han definido las **operaciones de influencia en la información**, y se refieren a ellas como los esfuerzos coordinados tanto de actores nacionales como extranjeros para influir en un público destinatario usando una serie de medios engañosos, como la supresión de fuentes de información independientes, unida a la desinformación; y la **injerencia extranjera en el espacio de la información**, a menudo realizada como parte de una operación híbrida más amplia, que puede entenderse como los esfuerzos coercitivos y engañosos para perturbar la libre formación y manifestación de la voluntad política de las personas por parte de un actor estatal extranjero o de sus agentes.

Para identificar los elementos básicos de las campañas de desinformación y evaluarlos de forma consistente, a continuación se relacionan diferentes componentes cuya combinación ayudará a caracterizar el fenómeno en cuestión: las tácticas, técnicas y procedimientos (TTPs) utilizados por los actores de la amenaza; el carácter manipulativo de la información, que es distinto de los patrones de comportamiento orgánicos y auténticos; la actividad en la zona gris, deliberadamente utilizada por la desinformación e injerencia extranjera en el espacio de la información; los valores, procedimientos y procesos políticos, teniendo en cuenta su potencial de afectar negativamente a los derechos y libertades fundamentales; la intencionalidad y la coordinación; así como la participación de actores estatales o no estatales y/o sus "proxies".

La emergencia en el siglo XXI de las plataformas digitales, las redes sociales, los sistemas de mensajería y la sociedad de la información, ha venido a transformar el panorama de la comunicación pública. En él también participan los usuarios que generan y comparten directamente contenidos con otros usuarios, alcanzando un alto grado de credibilidad, justificada o no, frente a los medios de comunicación y las entidades políticas, institucionales, económicas y sociales como fuente informativa (Badillo, 2019). Este nuevo contexto, tan abierto para la libertad de la información, ha facilitado también el desarrollo de campañas de desinformación que se sirven de la acelerada digitalización de los flujos de información para instrumentalizar, con fines espurios, los cambios en la intermediación mediática.

La posibilidad ofrecida por las plataformas digitales y redes sociales a sus usuarios de asumir una participación directa y activa como protagonistas en el debate público, creando y difundiendo contenido y opiniones, se presenta como un plus de democratización y de refuerzo de la personalidad del usuario que puede compartir sus contenidos directamente con más usuarios. De modo que, en este nuevo ecosistema comunicativo derivado de las nuevas

tecnologías, se multiplican los puntos de acceso a la información, ya sea de origen profesional o no[4].

Aparece entonces la figura de la narrativa que, dentro de contexto de la desinformación, incorpora elementos subjetivos, y que puede tener por finalidad moldear unos nuevos valores sociales, que en la vertiente política pueden subvertir los fundamentos clásicos de las sociedades democráticas o fomentar la desafección hacia la ciencia y la autoridad, como ha ocurrido en ciertos contextos durante la pandemia de la COVID-19 (Salaverría et al., 2020; Ricard y Medeiros, 2020; Germani y Biller-Andorno, 2021; Loomba et al., 2021).

La figura de la narrativa que, dentro de contexto de la desinformación, incorpora elementos subjetivos, y que puede tener por finalidad moldear unos nuevos valores sociales, que en la vertiente política pueden subvertir los fundamentos clásicos de las sociedades democráticas.

Las campañas de desinformación cuentan con dos tipos de actores, los que la propician (amenazas) y los que la combaten. Entre los primeros existe una amplia variedad de actores estatales o afines (*proxies*[5]), no-estatales (Giannopoulus y Smith, 2021), productores, distribuidores, internos o externos, individuales o colectivos, entre otros, que pueden converger entre ellos con motivaciones distintas (Sipher, 2018), y aprovechan la dificultad de atribución para actuar impunemente y fomentar la desestabilización y el desorden informativo (Wardle, 2020). Entre los segundos, y junto a los actores públicos, figuran actores privados como las plataformas digitales, organizaciones independientes de verificación (*fact-checkers*) y comunidades de expertos que autorregulan sus actividades y multiplican sus iniciativas para luchar contra las campañas de desinformación.

Las campañas de desinformación adaptan sus TTPs a los objetivos específicos perseguidos, aunque fundamentalmente basan sus estrategias

---

[4] Los agentes de la amenaza pueden aprovechar también este nuevo ecosistema para hacer un uso malicioso del mismo, en el que desplegar sus acciones. Como ejemplo, se puede encontrar los presuntos contactos a diversos influencers, Youtubers y bloggers franceses y alemanes por parte de una agencia de marketing vinculada con Rusia para llevar a cabo una campaña de descrédito de la vacuna Pfizer, a cambio de una compensación (Henley, 2021).

[5] La desinformación e interferencia extranjera puede ser llevada a cabo por gobiernos extranjeros o por actores extranjeros no estatales, incluidos los elementos que están directa y públicamente vinculados, financiados y controlados por ellos. Sin embargo, esta actividad también puede incluir el uso de los llamados "*proxies*" o "representantes", donde no se establece un vínculo visible públicamente, pero donde dichos actores están vinculados, financiados y controlados de manera encubierta.

en la falsificación (cuentas falsas o inauténticas) y en la coordinación en sus acciones para lograr sus objetivos. Se benefician de la dificultad de detectar y reaccionar frente a la multiplicación de actores y actuaciones que socavan de forma ambigua y gradual la estabilidad de los sistemas democráticos. En muchas ocasiones, incluyen operaciones de influencia mediante narrativas que deslegitiman la democracia y refuerzan el autoritarismo[6].

Las narrativas de las campañas de desinformación se diseñan en función de las audiencias para reforzar sus creencias y prejuicios o para cuestionar la percepción de los hechos o modificar opiniones.

Las narrativas de las campañas de desinformación se diseñan en función de las audiencias para reforzar sus creencias y prejuicios o para cuestionar la percepción de los hechos o modificar opiniones. La "propaganda participativa" (Rogers et al., 2019) hace que los destinatarios se sientan empoderados por la información que reciben y partícipes de una corriente de opinión dominante.

Las campañas de desinformación, para ser eficaces, precisan recursos técnicos y humanos especializados y persistentes. Algunos actores internacionales como la Federación Rusa y la República Popular China llevan a cabo campañas

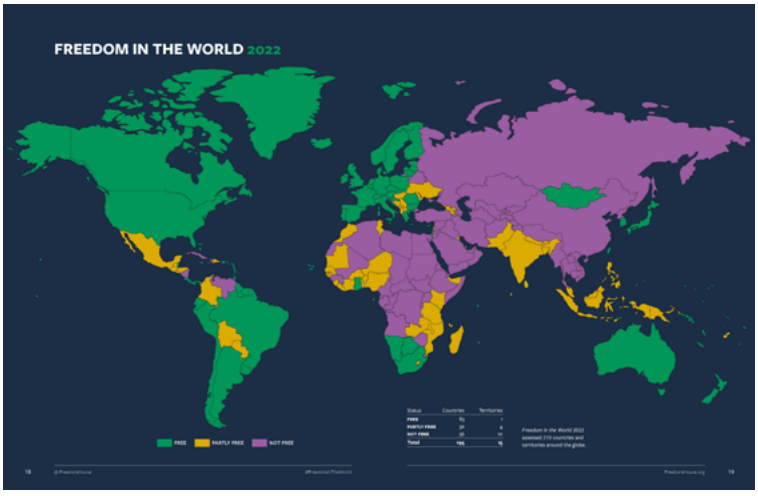


Foto 14: Índice de libertades en el mundo. (Repucci, S. y Slipowitz, A., 2022).

[6] Meta, dentro del GT2, diferencia entre desinformación (afirmaciones engañosas y falsas) de operaciones de influencia (acciones coordinadas e inauténticas para manipular el debate público con un objetivo estratégico). En el primer caso el foco se pone en el contenido y en el segundo en los actores y su comportamiento.

organizadas de desinformación como parte de las denominadas estrategias híbridas, por debajo del umbral de la guerra (zona gris), que pueden incorporan operaciones de información, subversión, presión económica, financiera o militar (Meta, 2021a; Bradshow y Howard, 2019; Bennett y Livingston, 2018; Krzyżanowski, 2019; Allcott y Gentzkow, 2017; A. Sánchez, 2020; Solsona, 2021).

Esos países, se sirven de las operaciones de influencia y/o campañas de desinformación para desestabilizar las instituciones de los países democráticos frente a sus poblaciones y disminuir la capacidad de atracción que pudieran tener para las suyas, desviando la atención de problemáticas internas. Como responsables de la lucha contra el fenómeno de la desinformación, frente a ellos se encuentran medios de comunicación, plataformas digitales, agencias de verificación, instituciones estatales, junto a empresas, organizaciones de la sociedad civil e individuos.

Las campañas de desinformación pueden sustentarse también en la creación de una red de medios propios (plataformas, dominios, webs y canales de comunicación) controlados por los propios productores de desinformación que canaliza y retroalimenta las vulnerabilidades socioeconómicas y políticas de un Estado con el objetivo de introducirlas en el debate en línea.

Las campañas de desinformación pueden sustentarse también en la creación de una red de medios propios, dado que la tecnología ha proporcionado nuevas posibilidades para que los actores externos interfieran en debates que son de ámbito doméstico. Esta red de medios propios, que se traduce en plataformas, dominios, webs y canales de comunicación controlados por los propios productores de desinformación que canaliza y retroalimenta -mediante la construcción de narrativas- las vulnerabilidades socioeconómicas y políticas de un Estado con el objetivo de introducirlas en el debate en línea.

LAS CAMPAÑAS DE DESINFORMACIÓN COMO PROBLEMA DE SEGURIDAD INTERNACIONAL

Las campañas de desinformación deben ser consideradas como un atentado contra la democracia en tanto que socavan el derecho a la libertad de información e intoxican la opinión pública. Habida cuenta de que sus efectos inmediatos o diferidos pueden alterar la percepción y reputación de las instituciones de los estados, de los medios de comunicación, de las empresas y de los ciudadanos, así como fomentar la alarma, confusión y polarización entre éstos últimos (Robinson et al., 2018). Sus efectos se ven potenciados por el uso malicioso que los actores detrás de las campañas de desinformación hacen de las plataformas de internet y las redes sociales consolidadas como espacios de debate público y desintermediado por los grandes medios de comunicación, en el que éstos participan, pero ya no como intérpretes únicos del mundo social y político.

Las campañas de desinformación deben ser consideradas como un atentado contra la democracia en tanto que socavan el derecho a la libertad de información e intoxican la opinión pública.

Las campañas desinformación representan una amenaza para la seguridad y cooperación nacional e internacional, por lo que los Estados deben dotarse de las estrategias y capacidades necesarias para detectar, analizar y contrarrestar las amenazas detrás de las campañas y desarrollar sistemas integrales de prevención y respuesta que disuadan a los actores hostiles de hacer uso de la desinformación, al limitar su eficacia e incrementar sus costes.

Por otro lado, la circulación tanto de desinformación como de información engañosa puede contribuir a crear tensiones sociales que pueden favorecer la incitación ilegal al odio, el fraude a los consumidores y riesgos para la salud como los evidenciados durante la "infodemia" del coronavirus a propósito del sistema de transmisión de la enfermedad y la vacunación para erradicar a ésta. De esta forma, la desinformación y/o información engañosa generada en torno a este asunto va encaminada a mermar la confianza en la ciencia, en la divulgación científica de los expertos y en la comunicación de las instituciones democráticas.

Precisamente, el uso malicioso de la tecnología para llevar a cabo acciones hostiles plantea desafíos que pueden afectar a la privacidad y la libertad

individual y favorecer el diseño de campañas de desinformación dirigidas a un público objetivo gracias a campañas patrocinadas o pagadas que buscan la segmentación y el *microtargeting*[7].

En este sentido, es importante señalar que existen casos de plataformas digitales que han desarrollado sistemas de control y transparencia para abordar estos riesgos mientras buscan mantener los beneficios de la publicidad sobre asuntos políticos y sociales, no sólo para que los partidos políticos puedan hacer llegar sus planteamientos a la ciudadanía de manera más efectiva, sino que también puedan hacerlo las organizaciones de la sociedad civil, ONGs y movimientos sociales, o candidatos y grupos políticos locales o menos conocidos o con recursos más modestos.

Entre estas buenas prácticas de plataformas digitales encontramos etiquetados visibles sobre anuncios políticos y sociales, procesos de verificación de identidad y residencia del anunciante, así como bibliotecas de anuncios de acceso público con información sobre el anunciante, el alcance y segmentación de la campaña publicitaria, así como la imposibilidad formal de llevar a cabo este tipo de campañas desde fuera del país para evitar injerencias extranjeras.

Adicionalmente, entre las medidas recomendables dirigidas a ofrecer un mayor control a los usuarios sobre el contenido patrocinado de carácter social y político que ven, se incluyen la posibilidad de que los usuarios

---

[7] La explotación de la capacidad de conocer, cada vez con mayor detalle, las preferencias, motivaciones y debilidades de los usuarios por medio de herramientas y estrategias digitales puede permitir a través de mensajes patrocinados orientar de manera personalizada los mensajes y focalizarlos directamente sobre la "audiencia objetivo" de cada campaña de desinformación. No obstante, la segmentación y el *microtargeting* no es factible en contenido orgánico (no patrocinado), y algunas plataformas en línea como Twitter, tienen prohibido la publicidad política, lo que imposibilita hacer llegar contenido político a los usuarios de manera segmentada.

puedan bloquear el contenido patrocinado de determinados anunciantes o la eliminación completa de los anuncios políticos o sociales[8].

Las actuaciones y estrategias por parte de los Estados contra las campañas de desinformación conocidas hasta ahora se centran en aquellas llevadas a cabo por terceros países, como parte de las operaciones de influencia y de interferencia extranjera (Salaverría-Aliaga, 2021). Pueden ser consideradas como parte de las amenazas híbridas contra estados democráticos y sus instituciones[9] y consisten en acciones coordinadas y sincronizadas para atacar de manera deliberada sus vulnerabilidades sistémicas. Estas operaciones pueden combinarse con un amplio rango de medios, como los ciberataques, el espionaje, la subversión o la coerción económica, entre otros de distinta naturaleza (híbridos).

La futura Estrategia debe ampliar su cobertura a la sociedad y sus grupos, a las empresas y los individuos, además de proteger los intereses e instituciones del Estado.

Sin embargo, las heridas más destructivas para la causa democrática se han producido en los últimos años mediante la convergencia entre actores externos e internos, estatales y no estatales. Los sistemas democráticos tienen que hacer frente a las acciones hostiles de grupos distintos que, con motivaciones diferentes convergen en campañas de

[8] La transparencia en la publicidad política y las páginas de redes sociales es fundamental para que los ciudadanos puedan conocer quién está tratando de influir en ellos. Plataformas como Facebook (Meta, 2021b) identifican de manera visible los anuncios políticos y sociales, así como la entidad que ha pagado por ellos. Las medidas de control incluyen un proceso formal de autorización donde los anunciantes deben demostrar quiénes son y dónde viven (estando formalmente prohibida la posibilidad de realizar una campaña de publicidad política o social desde fuera del país donde se muestra para evitar injerencias extranjeras). La biblioteca de anuncios de Facebook ofrece distinguiendo por países, durante 7 años, una base de datos de anuncios de acceso público en la que se pueden realizar búsquedas y que permite a periodistas, reguladores, grupos de vigilancia, investigadores, académicos y personas en general exigir responsabilidades a los anunciantes. Otras medidas de transparencia sobre las páginas en Facebook muestran información sobre cuándo se crearon, los cambios de nombre y la ubicación de los administradores de la página. También etiqueta a los medios de comunicación que creen que están total o parcialmente bajo el control editorial de su gobierno como medios controlados por el Estado. Los usuarios pueden también obtener información sobre por qué se les está mostrando un determinado anuncio a través de la herramienta ¿por qué estoy viendo este anuncio? Además de reforzar las medidas de transparencia, Facebook ofrece a los usuarios herramientas de control sobre los anuncios políticos y sociales que ven, pudiendo desactivar todos los anuncios de temas sociales, electorales o políticos de candidatos, u otras organizaciones que tengan el aviso de exención de responsabilidad política "Pagado por".

[9] Las amenazas híbridas son tratadas por, entre otros, el Centro de Excelencia de Comunicaciones Estratégicas de la OTAN (NATO StratCom CoE) y el Centro Europeo de Excelencia contra Amenazas Híbridas (Hybrid CoE).

desinformación, por lo que la futura estrategia no debe limitar su ámbito de actuación a la protección de los intereses e instituciones del Estado, sino que debe ampliar también su cobertura a la sociedad y sus grupos, las empresas y los individuos.

Las medidas que se describen para luchar contra las campañas de desinformación afrontan serios desafíos. Por un lado, los sistemas democráticos deben enfrentarse a la paradoja de que sus enemigos pueden emplear las facilidades que el propio sistema les confiere con el fin de sustituirlos por regímenes autoritarios y que, para hacerles frente, algunos actores podrían plantear la opción de limitar las libertades que pretenden defender[10].

Por otro lado, su capacidad de respuesta se ve mermada por la dificultad técnica y política de atribuir su autoría ya que los actores detrás de las campañas de desinformación explotan maliciosamente las posibilidades que ofrece la tecnología para contaminar el espacio informativo, valiéndose de la inteligencia artificial para generar perfiles falsos y/o simular la interacción orgánica en el debate público[11]; de la utilización de servicios de anonimización y cifrado de comunicaciones; de la creación de cuentas inauténticas para la distribución de contenido creando redes de comunidades opacas, así como las dificultades para recopilar evidencias que respalden una posible atribución.

A la dificultad de identificación del origen de las campañas se añade el de la atribución de responsabilidad de estas, lo que representa un desafío a la hora de adoptar medidas de disuasión, de amenaza o de respuesta que pueden conllevar una escalada, por lo que la futura Estrategia debería ir acompañada de un amplio listado de medidas (caja de herramientas) que permitiera flexibilizar su empleo en función del actor detrás de la campaña de desinformación. De esta manera, este enfoque variará si se trata de actores nacionales y extranjeros, puesto que las competencias de respuesta son diferentes.

La futura Estrategia debería ir acompañada de una caja de herramientas que permita flexibilizar su empleo en función del actor detrás de la campaña de desinformación.

[10] Para hacer frente a esta paradoja, Karl Loewenstein acuñó en 1937 el concepto de democracia militante, precisamente para justificar, en un contexto político y social distinto, la reacción de los Estados democráticos frente a este fenómeno.

[11] Simular un comportamiento humano para interactuar con otros usuarios en redes, con el objetivo, en la mayoría de las ocasiones, de provocar respuestas exacerbadas, polarizando el debate, y que puede ser en ambos extremos.

Debido a la novedad y a la sutileza del fenómeno, las sociedades abiertas se enfrentan a una falta de conocimiento y sensibilidad social que ha dificultado la aplicación de políticas de lucha contra este fenómeno.

Otros desafíos importantes para la lucha contra las campañas de desinformación tienen que ver con las distintas percepciones del riesgo, la variedad de marcos legales y sistemas mediáticos (Innerarity y Colomina, 2021). La percepción social determina la prioridad de la lucha contra la desinformación en las agendas públicas y, debido a la novedad y a la sutileza del fenómeno, las sociedades abiertas se enfrentan a una falta de conocimiento y sensibilidad social que ha dificultado la aplicación de políticas de lucha contra este fenómeno.

La necesaria alfabetización mediática e informacional tiene que incluir entre sus objetivos y medidas la concienciación política, social e individual de los riesgos y efectos que provocan la información engañosa y la desinformación. Dado que hasta el momento buena parte de nuestras percepciones sobre la desinformación y sus efectos se basan en intuiciones y no tanto en evidencias empíricas, resulta difícil encontrar métricas que pudieran reforzar la concienciación social, aunque se pueden encontrar estudios sobre la correlación con la polarización y otros problemas políticos (Zimmermann y Kohring, 2020; Ognyanova et al., 2020; Au et al., 2021).

Es difícil cuantificar el impacto concreto que una campaña tiene en el comportamiento político y social posterior, debido a las innumerables variables que intervienen en la conformación de las opiniones y acciones de los ciudadanos y a los sesgos y prejuicios preexistentes que facilitan la manipulación. Las campañas de desinformación más eficaces suelen pasar inadvertidas para el destinatario, lo que hace aún más difícil evaluar el impacto que ha tenido en las opiniones y actitudes de personas que ignoran que han sido sometidos a estas influencias hostiles.

La respuesta internacional

Las campañas de desinformación se han convertido en un problema de seguridad internacional en la medida que sus efectos afectan a la libertad y la seguridad de Estados y ciudadanos. El perjuicio público comprende amenazas contra los procesos democráticos políticos y de elaboración de políticas, así como contra los bienes públicos, como la protección de la salud, el medio ambiente o la seguridad de los ciudadanos. Riesgos que afectan a los ciudadanos y a la sociedad civil como posibles destinatarios de la información.

Las campañas de desinformación se han convertido en un problema de seguridad internacional en la medida que sus efectos afectan a la libertad y la seguridad de Estados y ciudadanos.

Sectores como el de los medios de comunicación o las instituciones se han visto afectados por las campañas de desinformación y/u operaciones de influencia en la UE o en Estados Unidos (Happer et al., 2019; Lee y Hosam, 2020; US Senate, 2020; Intelligence Community Assessment [ICA], 2017; ICA, 2021), aunque el efecto difiere en función de factores como la exposición a canales de segmentación, los niveles de educación, la cultura democrática, la confianza en las instituciones, la inclusividad de los sistemas electorales, la importancia de los recursos económicos en los procesos políticos y las desigualdades sociales y económicas.

En el ámbito multilateral, organizaciones como las de Naciones Unidas, la Organización para la Seguridad y Cooperación en Europa y la Organización de Estados Americanos se hicieron eco de que algunas medidas para frenar la desinformación pueden dañar la libertad de expresión de los individuos y de los medios de comunicación a través de una declaración conjunta sobre "Libertad de expresión y, 'noticias falsas', desinformación y propaganda" (Organization for Security and Co-operation in Europe [OSCE], 2017). A dicha declaración han seguido iniciativas no vinculantes de comités de expertos que se han multiplicado con la COVID-19 (Iniciativa "Verified") y la "infodemia" (United Nations General Assembly [UNGA], 2021; OSCE, 2021).

Dentro de la UE, la Comisión creó en 2015 un Grupo de Trabajo dentro del Servicio Europeo de Acción Exterior (East StratCom). En 2018 se convocó a un Grupo de Expertos de Alto Nivel independientes al que siguió la aprobación de la comunicación sobre la lucha contra la desinformación en línea (Comisión Europea, 2018b) y la del Plan de Acción Contra la Desinformación para proteger los sistemas democráticos de la Unión y las elecciones europeas (Comisión

Europea, 2018a). En 2019 se puso en marcha un sistema de alerta rápida y en 2020 se aprobó una comunicación acerca de la desinformación y el COVID-19 (Comisión Europea, 2020a) y el Plan de Acción sobre la Democracia Europea (Comisión Europea, 2020c). El Parlamento Europeo (2020) ha analizado la evolución de la intervención internacional y europea en un informe de su Comité de Libertades Civiles, Justicia y Asuntos Internos.

La Comisión ha impulsado la redacción de una nueva versión del Código de Buenas Prácticas sobre la Desinformación, sobre la base de las debilidades identificadas en la evaluación de la propia Comisión y ampliando el número y la naturaleza de los firmantes. El código original fue elaborado por plataformas digitales como Meta, Google o Twitter y representantes del sector de la publicidad en octubre de 2018 (Comisión Europea, 2018d). La Comisión presentó unas orientaciones para fortalecer el Código de buenas prácticas (Comisión Europea, 2021)[12], además de proponer el establecimiento de un marco de corregulación para dichos códigos, tal y como se indica en el borrador de la futura Ley de Servicios Digitales. Por otro lado, la Comisión ha ido tejiendo una red de centros como el Observatorio SOMA (Social Observatory for Disinformation and Social Media Analysis), el Centro de Transparencia del Código, así como el Observatorio Europeo de los Medios Digitales (EDMO) y sus 8 observatorios regionales[13].

Junto a las anteriores, ha proliferado la creación de buenas prácticas y observatorios de autorregulación, se han multiplicado las iniciativas de verificación (*fact-checking*)[14] y las herramientas de las plataformas digitales para luchar contra la desinformación. Asimismo, destaca la comunidad de investigación Credibility Coalition dedicada a crear estándares para compartir

[12] Se insta a reforzar, entre otras, áreas que impliquen una mejor desmonetización de la desinformación, el aseguramiento de la integridad de los servicios, el aumento de la cobertura de la verificación de datos y proporción de un mayor acceso de estos a los investigadores, o la creación de un marco de seguimiento más sólido. Asimismo, la Comisión Europea insta a los signatarios a que tengan en cuenta las recientes recomendaciones (European Regulators Group for Audiovisual Media Services [ERGA], 2021) del Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual.

[13] Para España y Portugal se ha creado el hub regional Iberifier (Iberian Digital Media Research and Fact Checking Hub) en el que participan 23 instituciones de ambos países.

[14] El International Fact Checking Network (IFCN) del Poynter Institute en 2015 acuñó un código que agrupa a la mayoría de las organizaciones. Entre otras, el Trust Project y sus indicadores de confianza; y la iniciativa Verified de NN.UU. Son también relevantes la plataforma First Draft de la Harvard 's Kennedy School, o los detectores de información engañosa Emergent, CrossCheck o Full Fact.

incidentes de desinformación y respuestas a ellos (esquema AMMIT)[15] y la Red Paneuropea para contrarrestar amenazas híbridas (EU-HYBNET).

Entre las iniciativas gubernamentales adoptadas destaca la institucionalización de la misión de detectar y denunciar las campañas de desinformación extranjeras como la mencionada East Stratcom Task Force de la UE; la creación de centros de análisis como el Hybrid CoE de Helsinki, el NATO StratCom CoE de Riga; o el Global Engagement Center del Departamento de Estado de EE.UU. También figura el desarrollo de normas para prevenir la desinformación (Francia, 2018), mejorar la resiliencia electoral (Ministerio de Asuntos Exteriores de Dinamarca, 2018), supervisar las redes sociales (Alemania, 2017), así como crear comisiones de investigación, fomentar la cooperación internacional o la alfabetización digital e informacional.

Entre las iniciativas gubernamentales adoptadas destaca la institucionalización de la misión de detectar y denunciar las campañas de desinformación extranjeras.

Por su parte, Francia modificó la regulación electoral (Francia, 2018) para luchar contra la manipulación de la información electoral y creó el denominado "Servicio de Vigilancia y Protección contra las Interferencias Digitales Extranjeras" en el seno de la Secretaría General de Defensa y Seguridad Nacional; con competencia en todo el territorio, junto a un Comité Ético y Científico compuesto por miembros de los distintos departamentos con competencias en la materia, y con la función de realizar un seguimiento de la actividad del nuevo servicio y elaborar un informe anual sobre su actividad (Francia, 2021). El Decreto encarga a la Secretaría General, en contacto con los departamentos ministeriales interesados, de "identificar las operaciones que impliquen, directa o indirectamente, a un estado extranjero o a una entidad no estatal extranjera, y que tengan por objeto la difusión artificial o automatizada, masiva y deliberada, por medio de un servicio de comunicación pública en línea, de alegaciones o imputaciones de hechos manifiestamente inexactos o engañosos que puedan atentar contra los intereses fundamentales de la nación", así como "dirigir y coordinar los trabajos interministeriales de protección contra este tipo de operaciones".

[15] La comunidad de investigación Credibility Coalition ha establecido el Grupo de Trabajo (Misinfosec) para describir y entender los incidentes de desinformación (Adversarial Misinformation and Influence Tactics and Techniques, AMMIT) según el esquema MITRE ATT&CK para ayudar a medir e identificar las TTPs utilizadas en el despliegue de campañas de desinformación e interferencia extranjera, así como para deducir el componente "intencionalidad" en las mismas.

Países Bajos (2019) ha elaborado una estrategia contra la desinformación estableciendo tres líneas de acción de Gobierno: prevención, el fortalecimiento de la posición informativa y, eventualmente, la estrategia de respuesta. Entre otras medidas, prevé el fortalecimiento de la resiliencia de los ciudadanos a través de las campañas de sensibilización y la mejora de alfabetización mediática, incluyendo una revisión integral del currículo educativo para la educación primaria y secundaria, la adaptación de la Administración pública a los desarrollos sociales y tecnológicos, el fortalecimiento de la preparación, formación y equipamiento de los titulares de cargos políticos, los contactos regulares entre el Ministerio de Educación, Cultura y Ciencia y el sector mediático y creadores de contenido profesionales. La transparencia política incluye un Código de Conducta de las plataformas sobre la publicidad electoral en línea.

La Agencia Sueca de Contingencias Civiles -MSB- (2018) elaboró un manual para comunicadores destinado a "contrarrestar las actividades de influencia de la información", así como las campañas de influencia de potencias extranjeras y de extremistas islamistas y se encarga de la alfabetización de los ciudadanos en materia de desinformación. La MSB viene organizando, desde 2015, un evento anual de capacitación como parte del Curso de Inteligencia Nacional Estratégica realizado por la Universidad Nacional de Defensa, reuniendo a funcionarios de alto nivel y capacitándolos en amenazas híbridas y desinformación.

Fuera de la UE, algunos países democráticos como Canadá (Canadian Secret Intelligence Service [CSIS], 2021) han reaccionado contra las campañas de desinformación con medidas para garantizar la integridad de los procesos electorales. Precisamente para evitar riesgos en las elecciones de 2019 de Canadá se adoptaron medidas como la consideración de algunas conductas desinformativas como delito electoral (si bien fue declarado inconstitucional tras las elecciones), la regulación de la propaganda en línea, un acuerdo de cooperación con las plataformas digitales, la creación de un grupo de coordinación de las agencias de seguridad frente a injerencias extranjeras o el fomento de iniciativas de alfabetización mediática entre otras.

Estados Unidos (2016) creó un Centro de Análisis y Respuesta en el Departamento de Estado para hacer frente a la desinformación. Más recientemente, Estados Unidos (2021) en su guía estratégica provisional para la Seguridad Nacional, define la desinformación como una de las prioridades de Seguridad Nacional y hace hincapié en la necesidad de colaborar con sus aliados en la lucha contra este fenómeno.

El Parlamento británico ha elaborado informes a partir de 2017 (UK Parliament, 2019) al que siguió una consulta pública durante 2019 (Reino Unido, 2020) y el actual borrador de seguridad en línea (Online Safety Bill) de 2021. En su estrategia de política exterior (Reino Unido, 2021) considera la desinformación como una amenaza estatal que pueden utilizar los actores no estatales y estatales para atacar a sus ciudadanos y explotar su espacio para su propio beneficio.

Finalmente, las plataformas digitales y redes sociales contribuyen a la lucha internacional contra las campañas de desinformación, por ejemplo, eliminando operaciones de influencia que buscan manipular el debate público a través de redes de actores inauténticos (comportamiento coordinado inauténtico), eliminando contenidos que violan sus normas, reduciendo significativamente la visibilidad de contenidos que, aunque no violan sus normas, han sido calificados como información engañosa por *fact-checkers* independientes; y/o informando a los usuarios con datos y contexto adicionales como, por ejemplo, creando centros de información que facilitan que la información oficial y/o de actores confiables llegue directamente a los ciudadanos a través de estas plataformas[16]; así como a las campañas de alfabetización mediática e informacional. Junto a ellas, las organizaciones independientes de verificación que comparten códigos de principios internacionales (International Fact Checking Network -IFCN-) se han convertido en otro actor importante en la lucha contra las noticias falsas y la desinformación (Hameleers y van der Meer, 2020).

[16] Véase el centro de información sobre COVID-19, el centro de información del clima o centros de información específicos para elecciones (piloto inicial en EEUU) en Facebook.

Relevancia para la seguridad nacional

En una sociedad digitalmente tan avanzada como la española[17], las denominadas amenazas híbridas crecen día a día y en numerosas ocasiones incluyen las operaciones de manipulación de la información como uno de sus mecanismos. En este nuevo contexto ya no sólo son objeto de ataques de desinformación en España, el Estado, las instituciones y las políticas públicas, sino también el sector privado, las empresas, los colectivos sociales y los individuos, con la consiguiente desestabilización social y pérdida de confianza en el sistema y en las instituciones que ello conlleva.

Todos pueden ser objetivos de una campaña de desinformación generada por Estados, grupos organizados, colectivos e individuos aislados y organizar campañas que promuevan la desestabilización democrática, social y económica o exploten tensiones nacionalistas, étnicas, raciales y religiosas.

En este sentido, podemos afirmar que todos pueden ser objetivos de una campaña de desinformación generada por Estados, grupos organizados, colectivos e individuos aislados con una capacidad de alcance impensable en otros tiempos y organizar campañas que promuevan la desestabilización democrática, social y económica o exploten tensiones nacionalistas, étnicas, raciales y religiosas.

La normalización de la desinformación, su capacidad de viralización y reproducción simultánea en distintos países y el aumento de los actores que ven la manipulación de la información como un factor geopolítico de interés creciente, son elementos que definirán las relaciones internacionales de los próximos años. Nuestro país se presenta como un lugar sensible en la circulación de desinformación al situarse por razones culturales, geográficas e idiomáticas como enclave y punto de encuentro con América Latina, pero también con Europa (Magallón-Rosa y Sánchez-Duarte, 2021). También lo es por el alto nivel de polarización política existente en España (Viciana et al., 2019).

Al igual que otros países, las elecciones en España también se han visto afectadas por la desinformación e información engañosa. EFE Verifica y Maldita.es han analizado la naturaleza de las 'desinformaciones' más

[17] España ocupa el noveno lugar de la UE, por delante de países como Alemania, Francia o Italia según el Índice de la Economía y la Sociedad Digitales (Comisión Europea, 2021b).

viralizadas en Internet (unos 30 ejemplos) durante las tres convocatorias electorales más recientes en España: las elecciones generales de noviembre de 2019 (Maldito Bulo, 2019), las elecciones al Parlament de Catalunya de febrero de 2021 (Maldito Bulo, 2021a) y las elecciones a la Asamblea de Madrid del mismo año (Maldito Bulo, 2021b).

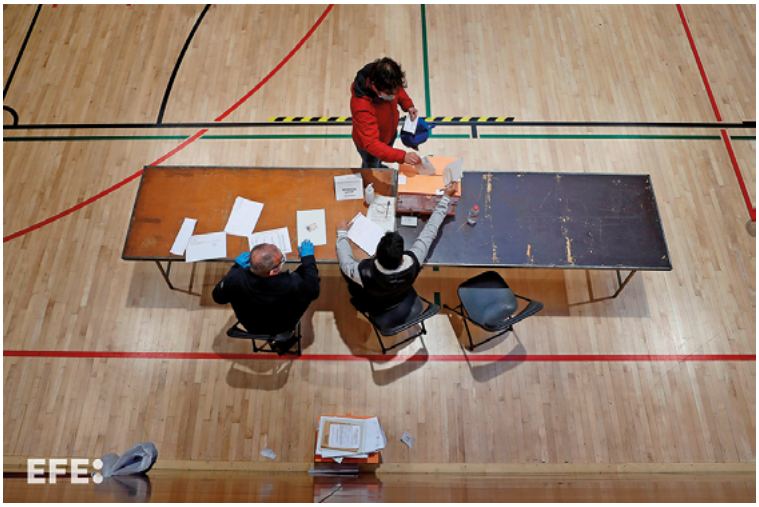


Foto 15: Un votante deposita su papeleta en las elecciones catalanas de 2021. EFE/Alberto Estévez

En este escenario es fácil que la desinformación y la información engañosa penetren con facilidad en el discurso mediático. El último informe Digital News Report España 2021 (Amoedo et al., 2021) destaca que la confianza de los ciudadanos españoles en las marcas periodísticas no es excelente. De hecho, no alcanza ni a la mitad de la población: sólo un 36% de españoles declara fiarse de la información general, aunque los medios siguen siendo la fuente principal de noticias. Esta confianza se mantiene y, según este informe, no disminuye por primera vez desde 2017[18]. Al mismo tiempo, también se debe considerar que la difusión de desinformación preocupa al 67% de los españoles. Por otro lado, los medios

La difusión de desinformación preocupa al 67% de los españoles.

[18] Una investigación comparativa a nivel internacional sitúa a España entre los países que muestran una confianza menor en los medios de comunicación y los profesionales del periodismo, si bien estos continúan siendo la fuente principal de noticias (Newman et al., 2020).

de comunicación tradicionales se enfrentan a los problemas de un mercado en transformación como consecuencia de las nuevas tecnologías, a una crisis en la financiación de sus actividades, a la pérdida de usuarios más jóvenes y a hábitos de consumo que afectan a la calidad de su producción periodística, pluralidad y sostenibilidad.

Del mismo modo, hay que tener en cuenta que España no cuenta con una evaluación oficial del fenómeno de las campañas de desinformación, y sus efectos, por lo que sería necesario su consideración futura en el marco de una Estrategia específica, tal y como se anunció por parte del Gobierno (P. Sánchez, 2020).

La Estrategia de Seguridad Nacional de 2017 identificó diferentes tipos de acciones hostiles como las actividades de desinformación e interferencias en procesos electorales.

En cuanto a la desinformación como concepto abordado en los documentos estratégicos nacionales, encontramos antecedentes en la Estrategia de Seguridad Nacional de 2017, la cual identificó diferentes tipos de acciones hostiles como las actividades de desinformación e interferencias en procesos electorales, acciones que representaban un desafío de grandes dimensiones tanto en lo que respectaba a los Gobiernos como a los ciudadanos, y consideró el ciberespacio como uno de los principales medios para realizar dichas actividades, pero no fijó objetivos ni líneas de acción contra esta problemática.

Por su parte, la Estrategia Nacional de Ciberseguridad de 2019 señaló a Internet como el campo de batalla donde la información y la privacidad de los datos son activos de alto valor, en un entorno de mayor competición geopolítica, reordenación del poder y empoderamiento del individuo, pero, del mismo modo, tampoco aportó medidas concretas.

Como continuación, la Estrategia de Seguridad Nacional de 2021 (ESN21) ha incluido como riesgo y amenaza a la Seguridad Nacional las campañas de desinformación, reconociendo el ámbito cognitivo como un espacio más en el que ejercer influencia. Por su potencial peligrosidad, señala las estrategias de desinformación de actores extranjeros, tanto estatales como no estatales, que desarrollan aparatos de propaganda con la intención de polarizar a la sociedad y minar su confianza en las instituciones. La ESN21 identifica, entre otras, a las campañas de

Estrategia de Seguridad Nacional de 2021 ha incluido como riesgo y amenaza a la Seguridad Nacional las campañas de desinformación, reconociendo el ámbito cognitivo como un espacio más en el que ejercer influencia.

desinformación como medio admisible de las estrategias híbridas llevadas a cabo por actores estatales y no estatales.

Por último, no podemos olvidar que la pandemia provocada por el coronavirus también ha sido foco importante de desinformación[19] e información engañosa. En este sentido y para contrarrestar estos dos fenómenos, los Ministerios de Sanidad y de Ciencia e Innovación (2018) pusieron en marcha un plan para la protección de la salud de las personas frente a las pseudoterapias, cuyo crecimiento se vio acelerado por la Covid-19. Asimismo, plataformas digitales como Twitter, Facebook o Instagram lanzaron centros de información sobre la Covid-19, haciendo llegar a la ciudadanía información oficial y fidedigna de fuentes gubernamentales u organismos internacionales como la Organización Mundial de la Salud.

Fuera de la esfera oficial, la percepción de las campañas de desinformación como riesgo y/o desafío estratégico se describe en las comparecencias de la Comisión Mixta de Seguridad Nacional (Ballesteros, 2021), o en estudios de centros de análisis (Milosevich, 2020; de Pedro, 2020) sin que exista todavía un desarrollo de la desinformación como área de conocimiento específica de las ciencias sociales (Sandulescu et al., 2020). Aunque el término de desinformación es relativamente reciente, este fenómeno ha sido estudiado desde las teorías de la comunicación durante el siglo XX desde diversas perspectivas (Romero Rodríguez, 2013).

Aunque el término de desinformación es relativamente reciente, este fenómeno ha sido estudiado desde las teorías de la comunicación durante el siglo XX desde diversas perspectivas.

La percepción de la desinformación como un riesgo trasciende a los Estados y en las distintas encuestas sociológicas, nacionales e internacionales, elaboradas en los últimos años se constata una creciente preocupación social e individual por la desinformación en sus diferentes formas[20]. Pero no

[19] El sitio web euvsdisinfo.eu publicó diversos informes elaborados por la División de Análisis de Información y Comunicaciones Estratégicas del Servicio Europeo de Acción Exterior (SEAE) enfocados en la "evaluación de las narrativas y la desinformación en torno a la pandemia de la COVID-19".

[20] Se mencionan los eurobarómetros Flash 464 de abril 2018 (el 88 % de los ciudadanos consideran que la desinformación es un problema en España), el Special Eurobarometer 503 de marzo de 2020 (el 66% afirma encontrarse con información falsa o que malinterpreta la realidad al menos una vez a la semana), el Eurobarómetro de 2021 (85% de los españoles consideran la desinformación como un problema para el país, y en un 86% para la democracia en general) y el Eurobarómetro especial 503 de diciembre de 2020 (el 62% afirma que los principales responsables de combatir la desinformación debían de ser los medios, 53% las autoridades públicas seguidos de las plataformas tecnológicas (48%).

hay evidencias de que los ciudadanos se muestren de acuerdo en controlar la información para frenar la expansión de la información engañosa[21].

Para dar respuesta a este fenómeno en España han surgido organizaciones, públicas y privadas, principalmente vinculadas al mundo del periodismo, que han impulsado emprendimientos para desenmascarar y combatir la desinformación e información engañosa. Se trata de los *fact-checkers*. En 2021 en nuestro país actúan organizaciones independientes (Maldita.es, Newtral, Verificat) o bien integradas en medios periodísticos mayores (EFE Verifica, Verifica RTVE) muchas de ellas colaboran, de manera independiente en su actuación, en los programas de lucha contra la información engañosa de las plataformas digitales y redes sociales[22].

La relevancia de las campañas de desinformación depende de la capacidad de medir sus efectos e impacto. Los problemas de medición afectan incluso a los actores que promueven este tipo de campañas, los cuales tienen incentivos para resolver a su favor esa falta de datos. Es habitual que estos tiendan a magnificar los resultados y apropiarse de la autoría de determinados sucesos como una forma de promocionarse ante sus superiores (Rid, 2020). Nuestra ceguera frente a los efectos de estas campañas debido a la dificultad

---

[21] El CIS realizó un barómetro durante los últimos días de marzo y primeros abril de 2020 en el que incluyó una pregunta que suscitó polémica tanto por su formulación (larga extensión y falta de claridad) como por su resultado. La pregunta 6 del estudio nº 3279 (Barómetro Especial de abril 2020) decía:
¿Cree usted que en estos momentos habría que prohibir la difusión de bulos e informaciones engañosas y poco fundamentadas por las redes y los medios de comunicación social, remitiendo toda la información sobre la pandemia a fuentes oficiales, o cree que hay que mantener libertad total para la difusión de noticias e informaciones?
La pregunta incluía simultáneamente cuatro contenidos susceptibles de ser prohibidos: bulos; informaciones engañosas; afirmaciones poco fundamentadas; informaciones provenientes de fuentes no oficiales. Esto hace imposible diferenciar entre quienes quizá apoyan la prohibición de algunos contenidos, pero no de otros. Conviene subrayar que, en principio, la protección constitucional de la libertad de información ampara totalmente la publicación de información poco fundamentada, así como la que procede de fuentes no oficiales, pero no necesariamente resulta equiparable con el derecho a difundir información engañosa y bulos.

[22] En la actualidad más de un centenar de entidades con el sello de la IFCN, cuatro de las cuales corresponden a España (Maldita.es, Newtral, Efe Verifica y Verificat). También cuenta con el sello de la IFCN el servicio en español de AFP Factual, unidad de verificación de la Agence France Presse, que realiza verificaciones sobre distintos países iberoamericanos, incluido España. También encontramos medios que utilizan aplicaciones de dominio público como TJ Tool, utilizada por el diario Público. Asimismo, varios medios periodísticos activan puntualmente equipos de verificación informativa con motivo de ciertos eventos informativos como elecciones o debates políticos y parlamentarios de especial importancia. Existen también otros colectivos y agencias verificadoras menores como La Chistera o SaludsinBulos.

de asignar una autoría en origen pero también a la dificultad de establecer relaciones causa efecto entre una campaña y su impacto real en la población, no sólo es preocupante porque podemos estar malgastando recursos en medidas irrelevantes sino, sobre todo, por el riesgo de que seamos incapaces de detectar los efectos contraproducentes de nuestras políticas de lucha contra la desinformación, en sus diferentes modos, en España.

El problema estructural de la medición no debe llevarnos a la resignación, sino al incremento de la financiación para seguir investigando sobre nuevas vías de indagación del impacto de las campañas de desinformación y de las políticas de neutralización de sus efectos[23]. Se trata ante todo de un desafío científico que puede ser resuelto parcialmente si se activa y respalda la creatividad de la comunidad de investigadores. Abordar nuestras lagunas analíticas es un requisito previo para conseguir que los responsables de formular políticas puedan identificar la forma correcta de actuar sobre el problema.

Aunque pudiera parecer que este tipo de incidentes solo requieren de una respuesta técnica, sus efectos demandan respuestas mucho más amplias e integrales que se mueven en los planos técnico, operacional y estratégico, que precisan la colaboración internacional y europea, así como el refuerzo y la coordinación nacional, en donde se incluye el tan necesario intercambio de información que apoye la toma de decisiones.

Por ello, se recomienda que España elabore una Estrategia Nacional de lucha contra las campañas de desinformación que incluya, entre otras, la identificación de las debilidades actuales, los límites, principios, objetivos y medidas para abordar este tipo de amenazas dentro del sistema y procedimientos de la Seguridad Nacional. Una Estrategia que deberá estar alineada y enmarcada en las iniciativas, comunicaciones y directrices europeas en esta materia.

Se recomienda que España elabore una Estrategia Nacional de lucha contra las campañas de desinformación que incluya, entre otras, la identificación de las debilidades actuales, los límites, principios, objetivos y medidas para abordar este tipo de amenazas dentro del sistema y procedimientos de la Seguridad Nacional.

[23] Las métricas del impacto se han desarrollado más para medir eventos puntuales que para medir impactos estructurales y a largo plazo sobre el sistema democrático (Norris et al., 2015; Rubio, 2018).

LÍMITES Y PRINCIPIOS DE LA ESTRATEGIA

En su evaluación de la práctica internacional y europea, en el Capítulo 2 se concluye que "se debe huir de una criminalización general del fenómeno por la grave dificultad de definir el mismo con la precisión necesaria para que la regulación sea efectiva". A lo anterior se añade la criminalización o la simple ilegalización de información porque sea falsa "es incompatible con el Derecho Internacional de los derechos humanos por otorgar a los Estados y sus autoridades la potestad discrecional de determinar la verdad o la falsedad acerca de temas socialmente relevantes". Las cautelas son más necesarias frente a las regulaciones restrictivas de naturaleza gubernativa o administrativa que frente a las de naturaleza judicial y, en todo caso, es recomendable la independencia de las autoridades regulatorias y la participación civil y judicial.

La criminalización o la simple ilegalización de información porque sea falsa es incompatible con el Derecho Internacional de los derechos humanos por otorgar a los Estados y sus autoridades la potestad discrecional de determinar la verdad o la falsedad acerca de temas socialmente relevantes.

Los límites de cualquier estrategia deben reconocer y proteger los derechos y obligaciones recogidos en la Constitución Española en su artículo 20: como el derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión y el de expresar libremente los pensamientos, ideas y opiniones. Es decir, nuestra Carta Magna reconoce la importancia de recibir una información cierta y contrastable, un concepto de "veracidad" cercano al de diligencia informativa y no exento de cierta controversia en la medida en que requiere ser contrastado[24]. Este derecho hace referencia a una "información verídica, comprobada y contrastada según los cánones de la profesión informativa" (López de Lerma Galán, 2018). Se hace esencial, por tanto, la práctica rigurosa de los principios periodísticos que asegure la calidad de los textos.

[24] Según el concepto de diligencia informativa, lo que da veracidad a una narración es que el periodista haya sido diligente en su contrastación y llegado a la convicción de que es razonablemente veraz.

Foto 16: Un ejemplar de la Constitución española en el Congreso de los Diputados. EFE/Chema Moya

Otro de los pilares de una sociedad democrática es la libertad de expresión recogida en el artículo 20.1.a) de la CE y que protege la expresión de pensamientos, ideas y opiniones que no están sujetas al criterio de veracidad, siendo ésta la principal diferencia con el derecho del art. 20.1.d). En esta línea, se debe diferenciar hechos y opiniones como señala la Constitución, ya que éstas últimas están exentas de demostración. Según lo expuesto en el Capítulo 2, "la jurisprudencia europea y española no llega a proteger el derecho a mentir, pero sí que teóricamente imposibilita el control de la verdad o mentira de las opiniones y dificulta mucho el control de la veracidad de las informaciones impregnadas de la libertad de expresión".

Es importante reseñar que no toda práctica comunicativa puede ampararse en estos preceptos. Estos derechos deben ejercerse con responsabilidad y están limitados por el resto de los derechos y libertades públicas como, por ejemplo, el honor, la intimidad, la protección de los datos, la rectificación, a la

infancia y la juventud, etc. De esta manera, en línea con el objeto de nuestro trabajo "la difusión de informaciones falsas, así como la transmisión de rumores o invenciones insidiosas haría decaer en la información su protección constitucional, pues en cierta manera está viciando el derecho a la información" (López de Lerma Galán, 2018). No obstante, y como se señala el Capítulo 2, incluso cuando algunos fenómenos de desinformación supongan el abuso del derecho a informar contra el sistema democrático de los artículos 17 CEDH y 54 de la Carta de Derechos fundamentales de la UE, su prohibición podría "seguir esta vía en casos muy evidentes y claramente vinculados a delitos de odio y siempre con la interpretación restrictiva que el TEDH exige respecto de estos delitos".

La desinformación es un problema que preocupa a la mayor parte de los españoles, aunque la manera de afrontarlo legalmente es delicada porque puede colisionar con otros derechos fundamentales, por lo que encontrará la resistencia de numerosos organismos, instituciones, partidos políticos y parte de la opinión pública; por eso, el éxito será directamente proporcional al mayor consenso logrado. En este sentido, la democracia se asienta en la garantía de un discurso público, garantía de libertad de reunión y asociación y libertad para expresar y hacer públicas opiniones. España defiende esta visión como nación plural y contribuye al esfuerzo conjunto de la comunidad internacional en este sentido. El acceso a una información veraz y de calidad es esencial en este marco para preservar la defensa de los valores y los principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos; especialmente en la protección de sus datos personales y su privacidad, su libertad de expresión es una prioridad. Dicho planteamiento exige trabajar con un enfoque multidisciplinar, que abarque aspectos más allá de los puramente técnicos.

La desinformación es un problema que preocupa a la mayor parte de los españoles, aunque la manera de afrontarlo legalmente es delicada porque puede colisionar con otros derechos fundamentales.

Las medidas que se deben adoptar para frenar las campañas de desinformación deben respetar la libertad de expresión, así como la libertad y pluralidad de los medios de comunicación, además del muy difícil equilibrio entre los derechos y libertades de los usuarios de las plataformas y las libertades de empresa y de expresión e información de las plataformas. Desde la perspectiva jurídico-normativa, cualquier respuesta penal o sancionadora al fenómeno desinformativo debe fundamentarse en conceptos muy concretos y restrictivos, más si cabe por su mayor impacto en libertades, derechos y

principios democráticos. Y, en todo caso, la regulación debería alinearse con la legislación europea mencionada: el Plan de Acción para la Democracia Europea, el Código de Buenas Prácticas en materia de desinformación y la Ley de Servicios Digitales.

Según lo apuntado en el Capítulo 2 una campaña de desinformación puede constituir, dependiendo de su alcance, naturaleza y efectos, una violación de los principios de soberanía o de no intervención o una amenaza, un uso de la fuerza, un ataque armado o una agresión contraria al Derecho Internacional. En respuesta, España puede adoptar las medidas necesarias para restaurar la legalidad y ejercer sus prerrogativas soberanas con relación a la atribución de las acciones y responsabilidades a un sujeto de Derecho Internacional o a cualquier agente a quien corresponda la autoría. La consideración de si la campaña de desinformación constituye o no una amenaza para la seguridad nacional se realizará conforme a la normativa nacional y podrá implicar el ejercicio del derecho a la legítima defensa individual y colectiva en los términos y condiciones prescritos en el art. 51 de la Carta de Naciones Unidas y conforme a los acuerdos suscritos en materia de asistencia mutua en el Tratado de la Unión Europea y en el marco de la Organización del Tratado del Atlántico Norte. En todo caso, la regulación de las medidas deberá arbitrar los mecanismos que aseguren el control, aunque sea a posteriori, de las medidas adoptadas por razones de seguridad nacional.

Una campaña de desinformación puede constituir, dependiendo de su alcance, naturaleza y efectos, una violación de los principios de soberanía o de no intervención o una amenaza, un uso de la fuerza, un ataque armado o una agresión contraria al Derecho Internacional.

Los principales riesgos para las libertades serían el control de la información por parte del poder y la falta de transparencia de los organismos públicos y privados. Las medidas propuestas en la Estrategia deben ser proporcionadas para no vulnerar el derecho a la libertad de expresión y la labor de los periodistas. Cualquier intento de criminalizar las informaciones falsas podría generar desconfianza en la información institucional, dificultad para acceder a la información contrastada y un efecto paralizante

Cualquier intento de criminalizar las informaciones falsas podría generar desconfianza en la información institucional, dificultad para acceder a la información contrastada y un efecto paralizante de la libertad de expresión.

de la libertad de expresión[25]. Las medidas de la futura Estrategia deben reforzar el papel de los medios, la libertad de expresión, el acceso a la información y la autorregulación. Por otra parte, y aunque se reconoce que los algoritmos facilitan las capacidades de detección y análisis, la experiencia humana debe jugar un papel preponderante en el proceso de decisiones.

La autorregulación[26] o la corregulación de las buenas prácticas seguirá siendo necesaria en la lucha contra la desinformación porque el Derecho no puede cubrir todas posibles manifestaciones, aunque tiene limitaciones como las que señala la Comisión Europea (2020b). Las plataformas y agencias de verificación contribuyen eficazmente a la lucha contra la desinformación, por lo que la futura Estrategia debería fomentar la mayor transparencia posible en sintonía con las propuestas de la Ley de Servicios Digitales de la UE y con otras acciones coordinadas con los otros Estados miembros a nivel UE[27] en aquello que fuera aplicable y/o extrapolable a las campañas de desinformación. Las exigencias de transparencia tendrían que ser aplicables también a todos los actores implicados, incluidos medios de comunicación.

En cuanto a los *fact-checkers*, para evitar posibles críticas de sesgo ideológico o de otro tipo, es fundamental que ofrezcan información sobre la metodología empleada, de forma que sean evidentes los criterios de selección y descarte de contenidos para su verificación, así como las garantías, derechos y, en su caso, la posibilidad de recurso que habilitan los mecanismos autorregulatorios. En este sentido, el estándar internacional más reconocido es el Código de Principios de la IFCN y sus compromisos auditados de apartidismo, transparencia metodológica y organizativa.

Debido al difícil equilibrio entre la lucha contra las campañas de desinformación y la protección de la libertad de expresión, se considera importante que la futura Estrategia impulse la visibilidad y alcance de fuentes de información legítimas, una mayor colaboración entre las plataformas digitales, los fact-checkers,

---

[25] Harlem Désir, representante de la OSCE para la libertad de los medios, criticó la penalización de la difusión de noticias erróneas por internet sobre el Covid-19 en Bulgaria con sanciones económicas (Désir, 2020).

[26] Debería basarse en códigos de conducta con compromisos adecuados, que fuera representativa por volumen de adheridos y contará con instrumentos independientes y eficaces para su monitorización y resolución de controversias.

[27] El proyecto First Draft está trabajando con Google y Meta para explorar si pudieran incorporar un código para detener la difusión de noticias falsas. Para estas plataformas ajustar los algoritmos no es como la censura, sino algo parecido a la carpeta de spam de un correo electrónico, esos correos siguen ahí, pero tienes que ir a tu carpeta de spam para buscarlos.

sociedad civil e instituciones, así como una adecuada formación en alfabetización mediática que otorgue a la ciudadanía las herramientas y conocimientos adecuados para pensar de manera crítica.

Es importante que la futura Estrategia impulse la visibilidad y alcance de fuentes de información legítimas, una mayor colaboración entre las plataformas digitales, los fact-checkers, sociedad civil e instituciones, así como una adecuada formación en alfabetización mediática.

Toda estrategia contiene un componente de comunicación que refuerza su credibilidad. La futura Estrategia deberá tener en cuenta la lección aprendida tras la aprobación del Procedimiento de actuación contra la desinformación (BOE, 2020), debido entre otras razones a la mala comunicación estratégica generada en su presentación, para evitar que se generen dudas en torno a una materia tan sensible para los derechos y libertades fundamentales. Adicionalmente, y por las mismas razones que llevaron a la creación del Grupo de Expertos que ha elaborado estas recomendaciones, la estrategia de desinformación debe asegurar la colaboración pública-privada en la elaboración y seguimiento de la Estrategia para que cuente con las mayores garantías posibles.

OBJETIVOS ESTRATÉGICOS Y LÍNEAS DE ACTUACIÓN

La lucha contra la desinformación se ha ido incorporando paulatinamente a las agendas de los Estados con el fin de garantizar la confianza de la sociedad, bajo el marco legal y los valores que rigen en las sociedades occidentales, que esencialmente se concretan en las ideas de democracia liberal concretada en el Estado de derecho, la defensa de las libertades públicas, los derechos fundamentales y singularmente el derecho a comunicar o recibir libremente información veraz y la libertad de expresión.

Para defender estos valores, la futura Estrategia debería incluir los siguientes objetivos estratégicos y desarrollarla mediante las líneas de actuación que corresponda:

- **Alfabetización mediática de la ciudadanía**. La información engañosa y la desinformación han existido siempre por lo que resulta ingenuo pensar que se podrá erradicar. Hay que aprender a convivir con ella y la solución no pasa exclusivamente por adoptar medidas tecnológicas sino por potenciar una conversación democrática. Ya que una parte de la población que comparte información falsa o errónea lo hace de manera involuntaria, se precisan iniciativas destinadas a generar conciencias críticas en los ciudadanos mediante la adquisición de nuevas habilidades intelectuales y digitales que les permitan cierta inmunidad hacia los contenidos tóxicos, sospechar de noticias de dudosa procedencia y evitar su propagación[28], así como capacitarse en metodologías para comprobar y/o verificar la información. Siendo la alfabetización mediática un objetivo estratégico, la futura Estrategia deberá incluir entre las líneas de actuación para alcanzarlo medidas que fomenten el desarrollo de una cultura

[28] Son interesantes iniciativas como “CTRL-F”, es el nombre de un programa ofrecido a través del sitio de alfabetización informativa CIVIX. El sitio fue creado por el Gobierno de Canadá y es una colección de vídeos, tutoriales y recursos que enseñan estrategias rápidas para investigar la información. Otros proyectos interesantes a nivel internacional son Snopes.com, es una fuente de comprobación de hechos basada en pruebas que ofrece recursos para animar a los lectores a realizar su propia comprobación de hechos. Analizan mitos urbanos, bulos y conspiraciones, rumores y desinformación en general. También la aplicación Verifiably, que fue creada por una ex-periodista política en línea de la CBC, Susana Mas, que también ha estado trabajando con el sector de la inmigración y los refugiados para enseñar sobre la desinformación.

ciudadana que facilite la detección de la desinformación como parte de la cultura más amplia de la seguridad nacional[29].

Según las conclusiones del Capítulo 3, la educación mediática debe incluirse como asignatura específica en el currículum académico de Primaria, Secundaria y Bachillerato[30]. En línea con el Plan Integral de Cultura de la Seguridad Nacional, se debe concienciar a los ciudadanos sobre la trascendencia del acceso a una información a través de campañas de información a nivel estatal. En estas campañas educativas e informativas se debería contar con las organizaciones profesionales y con un grupo de supervisión permanente.

- **Educación de los colectivos más vulnerables (jóvenes y mayores)[31].** En un contexto donde las dinámicas digitales permiten adaptar y viralizar la desinformación de manera rápida y coordinada, se consideran especialmente peligrosos los bulos que pretenden atacar la defensa de los derechos humanos o atentar contra la integridad y honor de determinadas personas por razones de sexo, raza, religión, orientación sexual, entre otros. La inclusión de estos colectivos más vulnerables como objetivo de la futura Estrategia se considera necesario por su mayor exposición.
- **Desarrollo de la desinformación como área de conocimiento**. La desinformación, en sus diferentes tipos, es un fenómeno que ha tenido un mayor desarrollo científico en el ámbito de la Comunicación que en el de otras ciencias sociales. Su desarrollo es imprescindible

---

[29] En el mismo sentido, sería conveniente que la Estrategia evalúe la creación de centros como la Agencia Federal para la Educación Cívica (Bundeszentrale Für Politische Bildung-BPD) creada en 1952 para concienciar a la población, desde la escuela hasta la universidad, con materiales y actividades diversas.

[30] El proyecto de ley orgánica de modificación de la LOE (LOMLOE) aprobada en el último pleno del Senado de 2020, apuesta por integrar la desinformación como parte de las competencias que los estudiantes menores de entre 6 y 12 años deben adquirir en su educación obligatoria como parte de la competencia número seis de Lengua Castellana. En esta, se insiste específicamente en que el alumno desarrolle las capacidades de "buscar, seleccionar y contrastar información procedente de dos o más fuentes, de forma planificada y con el debido acompañamiento" (Bocanegra y Giménez, 2021).

[31] El Poynter Institute lleva desde hace años apostando por los jóvenes, con la Teen Fact-Cheking Network, un proyecto de verificación de noticias hecho por y para adolescentes; y el MediaWise for Seniors, un programa de educación para mayores de 65 años. También son interesantes los newsgames, un género periodístico con un gran potencial para informar de forma práctica, didáctica y participativa. A través de la exposición de los usuarios a pequeñas dosis de desinformación, son capaces de reducir su predisposición a asumir contenidos falsos como ciertos. Algunos ejemplos son: Bad News creado por DROG y Universidad de Cambridge; Harmony Square; Troll Factory; i-Reporter (BBC); Guerra a la mentira (RTVE).

para medir la relevancia, alcance y efectos, por lo que se deben formular medidas de apoyo a la investigación científica y social en este campo. Las líneas de actuación de la futura Estrategia deberían impulsar estudios multidisciplinares en los que participen los actores implicados y cuenten con financiación y con acceso a bases de datos públicas de falsedades. Los estudios deben fomentar también la aplicación de métodos de investigación y marcos analíticos de análisis[32].

- **Transparencia y control.** La transparencia de las medidas adoptadas tanto por el sector público como por el sector privado, por humanos o por algoritmos es un principio esencial de la lucha contra la desinformación. Los gobiernos democráticos deben ser consecuentes con el hecho de que la transparencia es una de las principales armas a su disposición para la lucha contra la desinformación. Por el contrario, las barreras para el acceso a la información suelen ser utilizadas por las campañas desinformativas como el argumento que valida cualquiera de sus postulados, los cuales sólo deben fundamentarse en la especulación sobre los motivos de aquellos gobiernos que "ocultan algo". La forma de romper este círculo vicioso es evitar que la información pública circule de manera reactiva, cuando los manipuladores ya han contaminado las percepciones de la sociedad y resulta difícil revertir el daño.

  Tanto en el Capítulo 2 como en el Capítulo 4, se considera importante que la futura Estrategia dote al sistema de una gobernanza adecuada con participación y transparencia. Debería concretar la necesidad de elaborar informes de las acciones realizadas por los órganos públicos con responsabilidades en la materia y periodicidad y la publicidad activa de los mismos. La participación de agentes externos a la acción gubernamental en los mecanismos de transparencia y control es una garantía y el deber de secreto y confidencialidad que pueden requerir ciertas materias se puede asegurar jurídicamente. También debería aclararse si la información o documentación generada tiene en su caso una particular reserva y confidencialidad, que sólo debe darse en lo que sea necesario por razones de eficacia y seguridad y en el marco de la legislación aplicable.

---

[32] En el Capítulo 1 se identifican marcos analíticos y soluciones tecnológicas aplicables a la desinformación: la plataforma de código abierto OpenCTI, el marco AMITT (*Adversarial Misinformation and Influence Tactics and Techniques*) y el código abierto y gratuito STIX™ (*Structured Threat Information Expression*).

- **Colaboración público-privada**. El sector privado juega un papel relevante en la lucha contra la desinformación. Es el caso de gestores y propietarios de los medios de comunicación, las plataformas digitales, las agencias de verificación o las investigaciones de la academia. El principio de colaboración previsto en la Orden PCM/1030/2020 (Boletín Oficial del Estado [BOE], 2020) debe reforzarse en la futura Estrategia, tanto para su elaboración como en su desarrollo y seguimiento de esta. Se considera positiva la creación, existencia y participación de comités de expertos independientes que integren a la sociedad civil, a los sectores especialmente involucrados y a los ámbitos académico y judicial. También el desarrollo de instrumentos de colaboración entre el gobierno, la academia, la comunidad de verificadores de datos o las plataformas digitales que señala la misma Orden. Está colaboración podría concretarse en las líneas de actuación de la futura Estrategia en medidas como apoyar la sostenibilidad de los observatorios, el desarrollo de los programas de investigación y el apoyo a las iniciativas de los medios de comunicación en materia de lucha contra la desinformación[33].
- **Resiliencia electoral.** La protección de los procesos electorales debe ser otro objetivo de la futura Estrategia. Entre las posibles líneas de actuación para lograrlo, en el Capítulo 4 se propone la creación de un grupo de trabajo para el asesoramiento y seguimiento durante procesos electorales de carácter nacional, europeo, autonómico o local en España. También, la reforma de algunos artículos de la LOREG, sobre campañas institucionales en línea con las reformas de otros países y las nuevas medidas sobre contenido político patrocinado de la Comisión Europea. Recomienda a los partidos políticos reforzar su seguridad digital, la elaboración de un código de conducta y otras medidas de transparencia electoral. Para las plataformas sociales se proponen medidas para distinguir la publicidad electoral, transparencia, identificación de cuentas

[33] Esta era una de las conclusiones a las que llegó el estudio (Jeangène Vilmer, 2019) encargado por el gobierno francés para analizar las lecciones aprendidas del llamado "MacronLeaks,": el intento fallido por parte de actores rusos de interferir en el resultado de las elecciones presidenciales de 2017. Según este trabajo, una de las principales razones que explican que las filtraciones interesadas de la información robada al equipo de campaña de Enmanuel Macron tuvieron una escasa repercusión en la opinión pública, es precisamente que Francia contaba con un robusto ecosistema de medios de comunicación. A diferencia de otros países, los periódicos sensacionalistas y las webs de noticias "alternativas" tenían un escaso predicamento, lo que hizo que la prensa "seria" pudiese actuar como dique de contención frente una manipulación informativa externa que tenía el objetivo ilegítimo de interferir en el proceso electoral perjudicando al candidato centrista frente a su rival eurófoba y pro-rusa.

automatizadas (*bots*). Recomienda a los medios de comunicación y verificadores reforzar sus medidas de transparencia, rendición de cuentas y colaboración activa en las campañas de alfabetización mediática y digital que mejoren las competencias de los ciudadanos en el uso de la información en procesos electorales. Finalmente, recomienda a la sociedad civil disponer de una base de datos accesible sobre contenidos desinformativos de índole electoral, coordinar proyectos colaborativos de verificación durante procesos electorales y desarrollar mecanismos de alfabetización sobre los mismos, incluido el uso de juegos de simulación (*serious games).*

SISTEMA Y PROCEDIMIENTOS

Al igual que el GT2, el GT5 apoya la existencia de instituciones, órganos y funciones definidas normativamente en el ámbito gubernamental para "identificar, detectar y monitorear el fenómeno de la desinformación" y el refuerzo de la cooperación tanto entre el sector público como de éste "con la sociedad civil, la academia, las entidades de verificación de datos y el sector privado".

El sistema y procedimientos de lucha contra la desinformación a incluir en la futura Estrategia deben ser compatibles con los establecidos genéricamente en las estrategias de seguridad nacional y con los acordados específicamente en el Procedimiento de actuación contra la desinformación.

El sistema y procedimientos de lucha contra la desinformación a incluir en la futura Estrategia deben ser compatibles con los establecidos genéricamente en las estrategias de seguridad nacional y con los acordados específicamente en el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad nacional (BOE, 2020). Esta Orden, recurrida inicialmente, "no es una norma sustantiva o de conducta, sino de estructura o competencia" y "el procedimiento impugnado no incurre en ninguna restricción ni vulneración de los derechos fundamentales del artículo 20 de la CE", según la sentencia del Tribunal Supremo de 18 de octubre de 2021.

Dentro del sistema, el Consejo de Seguridad Nacional, el Comité de Situación y la Secretaría de Estado de Comunicación pueden incluir la desinformación dentro de sus funciones. En el caso de la Comisión Permanente contra la desinformación está prevista la participación de expertos que se podrían recabar a título individual o en representación de algún foro público o privado creado al efecto en la Estrategia, al igual que se ha articulado el Foro Nacional de Ciberseguridad dentro de la Estrategia Nacional de Ciberseguridad. De hecho, el propio Procedimiento incluye al sector privado y a la sociedad civil entre aquellos sectores que pueden cooperar con las autoridades competentes en el marco de la lucha contra la desinformación. Entre otros, menciona los medios de comunicación, las plataformas digitales, el sector tecnológico, el mundo académico o las organizaciones no gubernamentales a las que podrían añadirse las asociaciones y los colegios profesionales de periodistas, las organizaciones de verificación o los laboratorios de ideas.

El Procedimiento establece cuatro niveles de activación: 1) nivel técnico de atención, 2) nivel de coordinación, 3) nivel de decisiones y 4) nivel de gestión política en el marco del sistema de seguridad nacional. Dentro de estos niveles se considera importante la participación del sector privado en el desarrollo de metodologías de análisis y herramientas de respuesta frente a la desinformación, de forma que pueda contribuir eficazmente a una mayor capacidad de conocimiento del fenómeno dentro del Nivel 1 y con carácter permanente. Dentro de los otros niveles, que corresponden al ámbito de la autoridad pública, la presencia de algún representante del sector privado en la Comisión Permanente podría apoyar las decisiones públicas con elementos de análisis no oficiales en colaboración con el Foro al que representan. Una participación a la que se tiende en el marco de la Unión Europea, articulando una red de colaboración técnica en torno a centros especializados (EDMO) y observatorios regionales (IBERIFIER en el caso de España y Portugal).

Fuera del marco nacional, España ha seguido las orientaciones recogidas en el Plan de Acción de la UE y colaborado en la implementación de cada uno de los pilares que establece, así como con las distintas herramientas que ha ido desarrollando, tales como los Grupos de Trabajo Stratcom del SEAE y un sistema de alerta rápida para abordar las campañas de desinformación. En el sistema de la futura Estrategia debería incluirse la red de organizaciones con las que el sistema español deberá conectarse.

Tanto las estrategias como el procedimiento perciben la cooperación civil de modo reactivo, en caso de necesidad, mientras que la desinformación, por la relevancia expuesta debería superar ese umbral de recurso no inmediato. La participación privada puede aportar valor técnico al conocimiento y medición de los efectos de la desinformación, contribuir a campañas de alfabetización mediática y comunicación estratégica, mejorar la integridad de los procesos electorales y, sobre todo, a legitimar la acción de gobierno con un contrapeso civil que garantice que el ámbito de la lucha corresponsabiliza a toda la sociedad y no sólo al Estado y a las Administraciones y que la lucha y mecanismos de defensa y respuesta respetan los valores y derechos fundamentales de una sociedad democrática como la española.

La participación privada puede aportar valor técnico al conocimiento y medición de los efectos de la desinformación, contribuir a campañas de alfabetización mediática y comunicación estratégica, mejorar la integridad de los procesos electorales y, sobre todo, a legitimar la acción de gobierno con un contrapeso civil que garantice que el ámbito de la lucha corresponsabiliza a toda la sociedad y no sólo al Estado.

Por lo tanto, la futura Estrategia debería precisar el órgano y funciones para la colaboración público-privada en materia de desinformación, los hitos en que esta colaboración se debe sistematizar. Algunas posibles opciones como la participación en la elaboración y revisión de las estrategias, el seguimiento de las medidas adoptadas o el intercambio de iniciativas podrían residenciarse en la Comisión Mixta de Seguridad Nacional, en el posible Foro Nacional sobre desinformación o entre los órganos y niveles del sistema mencionado. Su inclusión en la primera estrategia de lucha contra las campañas de desinformación facilitaría el desarrollo de la colaboración experimentada en los grupos de expertos que han participado en la presente evaluación.

REFERENCIAS BIBLIOGRÁFICAS

Agencia Sueca de Contingencias Civiles (2018). *Countering Information Influence Activities*. https://www.msb.se/RibData/Filer/pdf/28698.pdf

Allcott, H. y Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election, *Journal Of Economic Perspectives*, 31(2), 211-236. https://doi.org/10.1257/jep.31.2.211

Alemania (2017). *Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG)* de 1 de septiembre (Federal Law Gazette I, p. 3352), https://germanlawarchive.iuscomp.org/?p=1245

Amoedo, A., Vara-Miguel, A., Negredo, S., Moreno, E., y Kuafmann, J. (2021). *Digital News Report España 2021*. https://www.digitalnewsreport.es/2021/infodemia-y-covid-gran-preocupacion-social-por-los-bulos-de-origen-politico/

Au, C.H., Ho, K.K.W., y Chiu, D.K. (2021). The Role of Online Misinformation and Fake News in Ideological Polarization: Barriers, Catalysts, and Implications. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-021-10133-9

Avaaz (2019). *Whatsapp Social Media's dark Web*. https://avaazimages.avaaz.org/Avaaz_SpanishWhatsApp_FINAL.pdf

Avaaz (2021). *Facebook's Climate of Deception: How Viral Misinformation Fuels the Climate Emergency*. https://avaazimages.avaaz.org/facebook_climate_misinformation.pdf

Badillo, A. (2019). *La sociedad de la desinformación: propaganda, «fake news» y la nueva geopolítica de la información*. Real Instituto Elcano. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/lengua+y+cultura/dt8-2019-badillo-sociedad-de-desinformacion-propaganda-fake-news-y-nueva-geopolitica-de-informacion

Ballesteros, M.A. (24 de mayo, 2021). *Estudio del fenómeno de la desinformación y de las fake news, con efectos disruptivos en la sociedad*. Comparecencia ante la Comisión Mixta de Seguridad Nacional, págs. 2-23, https://www.congreso.es/public_oficiales/L14/CORT/DS/CM/DSCG-14-CM-67.PDF

Bennett, W.L. y Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), 122-139. https://doi.org/10.1177/0267323118760317

Bocanegra, J. y Giménez, A. (11 de agosto, 2021). Educación pone los bulos y la desinformación como uno de los ejes de Lengua en Primaria. *El Confidencial*. https://www.elconfidencial.com/espana/2021-08-11/educacion-bulos-desinformacion-primaria_3225291/

Boletín Oficial del Estado. (2020). *Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobada por el Consejo de Seguridad Nacional* (BOE núm. 292, de 5 de noviembre de 2020, 96673-96680). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-13663

Bradshaw, S. y Howard, P.N. (2019). *The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation*. Oxford Internet Institute. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Canadian Secret Intelligence Service (2021). *Foreign Interference. Threats to Canada's Democratic Process*. https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-threats-to-canada%27s-democratic-process.pdf

Comisión Europea. (2018a). *Plan de Acción contra la Desinformación* (JOIN(2018) 36 final). https://data.consilium.europa.eu/doc/document/ST-15431-2018-INIT/es/pdf

Comisión Europea. (2018b). *La lucha contra la desinformación en línea: un enfoque europeo* (COM(2018) 236 final). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236&from=EN

Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías. (2018c). *A multi-dimensional approach to disinformation: report of the independent High level Group on fake news and online disinformation*. Publications Office. https://data.europa.eu/doi/10.2759/739290

Comisión Europea. (2018d). *Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

Comisión Europea. (2020a). *La lucha contra la desinformación acerca de la COVID-19: contrastando los datos* (JOIN(2020) 8 final). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020JC0008

Comisión Europea. (2020b). *Assessment of the Code of Practice on Disinformation. Achievements and areas for further improvement* (SWD(2020)180 final). https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement

Comisión Europea. (2020c). *Plan de Acción para la Democracia Europea* (COM(2020) 790 final). https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0790&from=ES

Comisión Europea. (2021). *Orientaciones de la Comisión Europea sobre el refuerzo del Código de Buenas Prácticas en materia de Desinformación* (COM(2021) 262 final). https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52021DC0262

Comisión Europea (2021b). Índice de la Economía y la Sociedad Digitales (DESI). https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/Posicionamiento-Internacional/Comision_Europea_OBSAE/Indice-de-Economia-y-Sociedad-Digital-DESI-.html

de Pedro, N. (2020). Crisis del Coronavirus. La desinformación del separatismo catalán como desafío estratégico para España, https://seguridadycultura.org/wp-content/uploads/2020/04/ISC_Desinfo-CAT_AFF.pdf

Désir, H. (15 de abril, 2020). COVID-19 response in Bulgaria should not curb media freedom, says OSCE Representative on Freedom of the Media. *Osce.* https://www.osce.org/representative-on-freedom-of-media/450193

European Regulators Group for Audiovisual Media Services (2021). *ERGA recommendations for the new code of practice on disinformation.* https://erga-online.eu/wp-content/uploads/2021/11/ERGA-RECOMMENDATIONS-2021_11.pdf

Estados Unidos (2016). *Countering Foreign Propaganada and Disinformation Act* (S. 3274). US Senate. https://www.congress.gov/bill/114th-congress/senate-bill/3274/text

Estados Unidos (2021). *Interim National Security Strategic Guidance*. The White House, Washington. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

Francia (2018). Ley Orgánica 2018-1202, de 22 de diciembre, sobre la *lutte contre la manipulation de l'information* (JORF n°0297 du 23 décembre 2018). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037847556

Francia (2021). Décret n° 2021-922, de 13 de julio de 2021, por el que se crea un servicio con competencia nacional denominado “servicio de vigilancia y protección frente a las injerencias digitales extranjeras” (JORF n°0162 del 14 de julio de 2021). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361

Germani, F. y Biller-Andorno, N. (2021). The anti-vaccination infodemic on social media: A behavioral analysis. *PLOS ONE*, 16(3). https://doi.org/10.1371/journal.pone.0247642

Giannopoulos, G. y Smith, H. (Eds.) (2021). *The Lanscape of Hybrid Threats. A Conceptual Model*. Publications Office of the European Union, Luxembourg. https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

Hameleers, M. y van der Meer, T.G.L.A. (2020). Misinformation and polarization in a high-choice media environment: How effective are political fact-checkers? *Communication Research*, *47*(2), 227-250. https://journals.sagepub.com/doi/pdf/10.1177/0093650218819671

Happer, C., Hoskins, A., y Merrin, W. (2019), *Trump’s Media War*. Palgrave Macmillan, Cham.

Henley, J. (25 de mayo, 2021). Influencers say Russia-linked PR agency asked them to disparage Pfizer vaccine. *The Guardian*. https://www.theguardian.com/media/2021/may/25/influencers-say-russia-linked-pr-agency-asked-them-to-disparage-pfizer-vaccine

Innerarity, D. y Colomina, C. (2020). La verdad de la democracia algorítmica. *Revista CIDOB d’Afers Internacionals*, 124, 11-23. https://doi.org/10.24241/rcai.2020.124.1.11

Intelligence Community Assessment. (2017). *Assessing Russian Activities and Intentions in Recent US Elections*. Office of the Director of National Intelligence. National Intelligence Council. United States of America. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Intelligence Community Assessment. (2021). *Foreign Threats to the 2020 US Federal Elections.* National Intelligence Council. United States of America. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

Jeangène Vilmer, J.B. (2019). *The “#Macron leaks” operation: a post-mortem*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/

Krzyżanowski, M. (2019). Brexit and the imaginary of 'crisis': a discourse-conceptual analysis of European news media. *Critical Discourse Studies*, 16(4), 465-490. https://doi.org/10.1080/17405904.2019.1592001

Lee, T. y Hosam, L. (2020). Fake News Is Real: The Significance and Sources of Disbelief in Mainstream Media in Trump's America. *Sociological Forum,* 35(S1), 996-1018. https://doi.org/10.1111/socf.12603

Loomba, S., de Figueiredo, A., Piatek, S.J., de Graaf, K., y Larson, H.J. (2021). Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA. *Nature Human Behaviour*, 5, 337-348. https://doi.org/10.1038/s41562-021-01056-1

López de Lerma Galán, J. (2018). El derecho a recibir información veraz en el sistema constitucional. El ejercicio profesional del periodismo como garantía democrática. *Estudios de Deusto* 66(2), 435-459. http://dx.doi.org/10.18543/ed-66(2)-2018pp435-459

Magallón-Rosa, R., y Sánchez-Duarte, J.M. (2021). Information verification during COVID-19. Comparative analysis in Southern European Countries. *Thematic dossier International Relations and Social Networks*. https://observare.autonoma.pt/janus-net/wp-content/uploads/sites/2/2021/07/EN_International-Relations-and-Social-Networks_art10.html

Maldito Bulo (18 de mayo, 2019). 15 bulos sobre pucherazo o fraude electoral en las elecciones del 28ª que te están intentando colar. *Maldita*. https://maldita.es/malditobulo/20190518/11-bulos-sobre-un-pucherazo-o-fraude-electoral-en-las-elecciones-del-28a-que-te-estan-intentando-colar/

Maldito Bulo (15 de febrero, 2021a). Bulos y desinformaciones que te están intentando colar sobre las elecciones catalanas del 14 de febrero. *Maldita*. https://maldita.es/malditobulo/20210215/bulos-desinformaciones-intentado-colar-elecciones-catalanas-14-febrero/

Maldito Bulo (24 de marzo, 2021b). 53 bulos y desinformaciones sobre las elecciones a la Comunidad de Madrid del 4-M y sus candidatos". *Maldita*. https://maldita.es/malditobulo/20210504/bulos-desinformaciones-elecciones-comunidad-madrid-4-mayo

Mayoral, J., Parratt, S., y Morata, M. (2017). Desinformación, manipulación y credibilidad periodísticas: una perspectiva histórica. *Historia y comunicación social*, 24(2), 395-409. https://doi.org/10.5209/hics.66267

Meta. (2021a). The State of Influence Operations 2017-2020. https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf.

Meta. (2021b). *Anuncios sobre temas sociales, elecciones o política*. https://www.facebook.com/business/help/issuesandpolitics

Ministerio de Asuntos Exteriores de Dinamarca. (2018). *Strengthened safeguards against foreign influence on Danish elections and democracy*. https://www.fmn.dk/en/news/english/strengthened-safeguards-against-foreign-influence-on-danish-elections-and-democracy/

Newman, N., Fletcher, R., Schulz, A., Andi, S., y Nielsen, R.K. (2020). *Reuters Institute Digital News Report 2020*. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/digital-news-report-2018.pdf

Nielsen, R.K. y Graves, L. (2017). *News you don't believe: Audience perspectives on fake news*. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-10/Nielsen%26Graves_factsheet_1710v3_FINAL_download.pdf

Ministerios de Sanidad, Consumo y Bienestar Social y de Ciencia, Innovación y Universidades (2018). *Plan para la protección de la salud frente a las pseudoterapias*. https://www.mscbs.gob.es/gabinetePrensa/notaPrensa/pdf/20181141118135247771.pdf

Milosevich, M. (2020). *¿Por qué hay que analizar y comprender las campañas de desinformación de China y Rusia sobre el COVID-19?* (ARI 58/2020). Real Instituto Elcano. https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari58-2020-milosevich-analizar-y-comprender-campanas-desinformacion-china-rusia-covid-19.pdf

Norris, P., Frank, R.W., y Martínez i Coma, F. (2015) *Contentious Elections: From Ballots to Barricades*. Routledge, London-New York.

Ognyanova, K., Lazer, D., Robertson, R. E., y Wilson, C. (2020). Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. *Harvard Kennedy School (HKS) Misinformation Review*, 1(4). https://doi.org/10.37016/mr-2020-024

Online Safety Bill (2021). *Draft Online Safety Bill*. Presented to Parliament by the Minister of State for Digital and Culture by Command of Her Majesty May 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

Organization for Security and Co-operation in Europe. (2017). *Joint Declaration on Freedom of Expression and "Fake News", disinformation*

and Propaganda. https://www.osce.org/files/f/documents/6/8/302796.pdf

Organization for Security and Co-operation in Europe. (2021). *Second Experts Meeting on Disinformation and media self-Regulation.* OSCE Representative on Freedom of the Media*.* https://www.osce.org/Node/490340

Países Bajos (2019). *Carta al parlamento sobre el compromiso político para proteger la democracia contra la desinformación*. https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/18/actielijnen-tegengaan-desinformatie

Países Bajos (2020), Código de Conducta para mejorar la transparencia política firmado por el Parlamento holandés y las plataformas digitales (https://www.idea.int/sites/default/files/news/news-pdfs/Dutch-Code-of-Conduct-transparency-online-political-advertisements-EN.pdf).

Parlamento Europeo. (2020). *Refuerzo de la libertad de los medios de comunicación: protección de los periodistas en Europa, discurso del odio, desinformación y papel de las plataformas* (Resolución 2020/2009(INI)). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0320_ES.pdf

Reino Unido (2020). *Online Harms White Paper: Full government response to the consultation*. Home Office y Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

Reino Unido (2021). *Global Britain in a competitive age*. *The Integrated Review of Security, Defence, Development and Foreign Policy.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

Repucci, S. y Slipowitz, A. (2022). Freedom in the world 2022: The Global Expansion of Authoritarian Rule. *Freedom House*.

Ricard, J., y Medeiros, J. (2020). Using misinformation as a political weapon: COVID-19 and Bolsonaro in Brazil. *Harvard Kennedy School (HKS) Misinformation Review,* 1(2). http://nrs.harvard.edu/urn-3:HUL.InstRepos:42661741

Rid, T. (2020). *Active Measures. The Secret History of Disinformation and Political Warfare*. Farrar, Straus & Giroux.

Robinson, L., Helmus, T., Cohen, R., Nader, A., Radin, A., Magnuson, M., y Migacheva, K. (2018). *Modern Political Warfare. Current Practices and Possible Responses*. Rand Corporation. https://doi.org/10.7249/RR1772

Rodríguez Pérez, C. (2019). No diga fake news, di desinformación: una revisión sobre el fenómeno de las noticias falsas y sus implicaciones. *Comunicación*, (40), 65-74. https://doi.org/10.18566/comunica.n40.a05

Rogers, Z., Bienvenue, E., y Kelton, M. (1 de mayo, 2019) The New Age of Propaganda: Understanding Influence Operations in the Digital Age. *War on the Rocks*. https://warontherocks.com/2019/05/the-new-age-of-propaganda-understanding-influence-operations-in-the-digital-age/

Romero Rodríguez, L.M. (2013). Hacia un estado de la cuestión de las Investigaciones sobre desinformación / misinformación. *Correspondencias & Análisis*, 3, 319-342. http://dx.doi.org/10.24265/cian.2013.n3.14

Rubio Núñez, R. (2018). Los efectos de la posverdad en la democracia. *Revista De Derecho Político*, 1(103), 191–228. https://doi.org/10.5944/rdp.103.2018.23201

Salaverría, R., Buslón, N., López-Pan, F., León, B., López-Goñi, I., y Erviti, M. C. (2020). Desinformación en tiempos de pandemia: tipología de los bulos sobre la Covid-19. *Profesional de la información*, 29(3). https://doi.org/10.3145/epi.2020.may.15

Salaverría-Aliaga, R. (2021). Entender y combatir la desinformación sobre ciencia y salud. *Ministerio de Ciencia e Innovación*. https://hdl.handle.net/10171/60223

Sandulescu Budea, A.M., Rubira García, R., y Videla Rodríguez, J.J. (2020). La desinformación como objeto de estudio en España: un balance teórico-metodológico de las revistas del campo científico. C*omunicación y Diversidad. Libro de comunicaciones del VII Congreso Internacional de la Asociación Española de Investigación de la Comunicación*, 369-384. https://aeicvalencia2020.org/wp-content/uploads/2021/01/Libro-de-Comunicaciones-VII-Congreso-Internacional-de-la-AE-IC-Valencia-2020.pdf

Sánchez, A. (10 de junio, 2020). La UE señala a Rusia y China como instigadoras de campañas de desinformación en plena pandemia. *El País*. https://elpais.com/internacional/2020-06-10/la-ue-senala-a-rusia-y-china-como-instigadoras-de-campanas-de-desinformacion-en-plena-pandemia.html

Sánchez, P. (4 de enero, 2020). *Discurso de la primera sesión de investidura*. Congreso de los Diputados, pág. 31. https://www.lamoncloa.gob.es/presidente/intervenciones/Documents/2020/20200104%20PG%20Discurso%20investidura%20(2).pdf

Sipher, J. (13 de Agosto, 2018). Convergence Is Worse Than Collusion, *The Atlantic*. https://www.theatlantic.com/ideas/archive/2018/08/convergence-is-worse-than-collusion/567368/

Sixto García, J., Soengas Pérez, X., Rodríguez Vázquez, A.I., Vázquez Herrero, J., y López-García, X. (2021). Percepción social del periodismo en España. *AdComunica,* (22), 191-210. https://doi.org/10.6035/2174-0992.2021.22.11

Solsona, M.A.B. (2021). La UE frente a la desinformación de China y Rusia durante la COVID-19. La necesidad de una mayor proactividad narrativa europea a nivel internacional. *Thematic dossier International Relations and Social Networks*. https://doi.org/10.26619/1647-7251.DT21.6

Tandoc Jr., E.C., Lim, Z.W., y Ling. R. (2018). Defining ”Fake News”. A typology of scholarly definitions. *Digital Journalism,* 6(2), 137-153. https://doi.org/10.1080/21670811.2017.1360143

Teruel Rodríguez, L. (2016). El impacto de la crisis política y económica sobre la polarización de los medios españoles. *Historia y comunicación social*, 21(1), 203-220. https://doi.org/10.5209/rev_HICS.2016.v21.n1.52692

UK Parliament (2019). *Disinformation and “fake-news”. Final Report: Government Response to the Committee’s Eighth Report*. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/2184/218402.htm

United Nations General Assembly, (27 de abril, 2021). *Delegates in Information Committee Call for Expanded United Nations Multilingual Communications Strategy to End Rapid Spread of Disinformation Worldwide*. Comité de Información, 43 sesión, 3 reunión. https://www.un.org/press/en/2021/pi2293.doc.htm

US Senate, Select Committee on Intelligence (2020). *Russian active measures campaigns and interference in the 2016 U.S. Election*. *Report Volumes I-V*. .S. Government Publishing Office. https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures

Valaskivi, K. (2018). *Beyond Fake News: Content Confusion and Understanding the Dynamics of the Contemporary Media Environment*. Hybrid CoE Strategic Analysis. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-5-Valaskivi.pdf

Viciana, H., Hannaikainen, I.R., y Gaitan Torres, A. (2019). The Dual Nature of Partisan Prejudice: Morality and Identitty in a Multiparty Systema. *Plos one*, 14(7). https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0219509

Wardle, C. (2020). *Comprender el desorden informativo*. *First Draft News*. https://firstdraftnews.org/wp-content/uploads/2020/07/Information_Disorder_Digital_AW_ES.pdf?x35395

Wardle, C. y Derakhshan, H. (2017). *Information disorder toward an interdisciplinary framework for research and policymaking* (DGI(2017)09), Consejo de Europa. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Weedon, J., Nuland, W., y Stamos, A. (2017). *Information Operations and Facebook*. Facebook. https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf

Zimmermann, F. y Kohring, M. (2020). Mistrust, disinforming news, and vote choice: A panel survey on the origins and consequences of believing disinformation in the 2017 German parliamentary election. *Political Communication*, 37(2), 215-237. https://doi.org/10.1080/10584609.2019.1686095