

DERECHOS FUNDAMENTALES Y CONTROL DE LA DESINFORMACIÓN: SOLUCIONES Y NUEVOS PROBLEMAS

Raquel Seijas
Universidad de Málaga.

Resumen

Durante las últimas décadas las mayores amenazas a la libertad de expresión, acceso a la información y a otros derechos fundamentales provienen: de la propagación de desinformación y de la intromisión y mercantilización de datos personales. Si una parte de la solución para luchar contra la desinformación pasa por crear instrumentos de control que pueden vulnerar o suponer una intromisión en la privacidad y en la libertad de expresión, las soluciones comienzan a ser un problema.

Esta investigación tiene un doble objetivo: por un lado, hablar brevemente de las medidas que han puesto en marcha desde la Unión Europea (UE) y el gobierno español para eliminar la desinformación y proteger la privacidad; y por otro, comprobar si las iniciativas que se han puesto en marcha son compatibles con la libertad de expresión e información, la privacidad y con el derecho a acceder a una información diversa.

Introducción

No es una novedad la desinformación, pero ha sido en esta última década cuando se ha hablado más, a todos los niveles, de este fenómeno. La responsabilidad de que la desinformación esté en el centro de muchos debates, y sea objeto

de preocupación para muchos ciudadanos europeos, se debe a la rapidez con la que se difunde y a su apoyo en herramientas tecnológicas. Estas herramientas son capaces de desafiar a las legislaciones más potentes, y de convertir la transmisión de información en un proceso con múltiples aristas carente de la finalidad y propósito original. La transmisión y el acceso a la información es la base de los sistemas democráticos y parte vital en el desarrollo de la opinión pública, la conciencia democrática y crítica de la ciudadanía.

La difusión de desinformación está convirtiéndose en un arma estratégica: las campañas para desinformar son globales y afectan a procesos políticos democráticos, pudiendo influir en la seguridad de los Estados. Pero sobre todo, llama la atención la tensión provocada entre las herramientas para limitar la desinformación y el impacto que el control de la desinformación está teniendo en derechos fundamentales, como el de acceso a la información o la libertad de expresión.

En algunas de las iniciativas de control de la desinformación se aprecia una limitación, consciente o no, de algunos derechos fundamentales, junto con la aparición de censura y de una mayor autocensura.

Para saber controlar la desinformación hay que identificar, de manera precisa, cuáles son las amenazas reales que lleva aparejada la transmisión de información, lo que facilitará la búsqueda de soluciones. Además, hay que conocer el espacio y las herramientas tecnológicas usadas para transmitir desinformación, quién o quienes la difunden y para qué. Las iniciativas contra la desinformación, que limitan los derechos fundamentales, no van a evitar su difusión si se desconoce el contexto en el que se mueve y su objetivo.

Los Estados o entidades supranacionales han observado la dificultad de controlar o evitar la desinformación sin atropellar derechos como la libertad de expresión, libertad de información, acceso a la información, o el derecho a la privacidad. Pero es difícil determinar cuáles son las políticas correctas si no se aplican iniciativas en las que en su eje cen-

tral tengan la alfabetización mediática, se evite el dominio tecnológico por parte de algunas empresas y se limite la utilización de nuestros datos, junto con el convencimiento de que las soluciones han de ser adaptativas al medio tecnológico, principal transmisor de la desinformación.

Es complejo seguir el ritmo vertiginoso de la tecnología, aún así los Estados legislan desde el punto de vista de limitar riesgos, pero pueden excederse porque el desafío de frenar la desinformación es excesivamente complejo. Desde que se identifica la desinformación como problema, conceptos como el de la seguridad nacional se han utilizado para limitar actividades relacionadas con la información o las movilizaciones ciudadanas. Al no tratarse de una amenaza tradicional y no ser nada homogénea, la manera de abordar el problema debe ser similar. A pesar de la capacidad de la UE, las iniciativas han sido tardías y han aparecido cuando la desinformación amenazaba los sistemas democrático-occidentales y sus procesos electorales. Pero, además, la desinformación puede determinar políticas de gobiernos de países desarrollados respecto a Estados más frágiles, condicionando sus decisiones; todo por la difusión de desinformación que, paradójicamente, se realiza desde países económicamente superiores (Merlos, A., 2018). La tecnología ha transformado la operativa en la estructura general de la esfera pública democrática: la interferencia de la desinformación en las campañas y la manipulación de la opinión pública, ponen de relevancia las dificultades para enfrentarse a este hecho a través de la legislación nacional e internacional y las iniciativas auto regulatorias (Chulvi, C.P., 2018).

Metodología

Esta comunicación es producto de una investigación descriptiva sobre las medidas e iniciativas europeas para frenar

la desinformación y las implicaciones que estas pueden tener sobre los derechos fundamentales. El trabajo se sustenta, además, en la revisión y análisis documental, tanto de trabajos científicos sobre desinformación y derechos fundamentales como en normativa europea y española. También ha sido esencial la recopilación de análisis sobre el contexto, los efectos de la desinformación y su impacto sobre derechos fundamentales que han realizado instituciones y diarios especializados de prestigio. Con esta metodología, se obtienen resultados que permiten valorar los efectos de las acciones emprendidas sobre los derechos fundamentales, alertando y orientando sobre la peligrosidad que supone la elaboración de medidas que pueden incurrir en el ejercicio de nuestros derechos fundamentales.

Desarrollo

Algunas medidas y acciones de la UE frente a la desinformación

En este apartado se presentan, a modo de síntesis, medidas e iniciativas de la UE para abordar el fenómeno de la desinformación.

La UE ya conocía el efecto de la desinformación en el ámbito financiero, cuestión que queda recogida en el Reglamento UE nº 596/2014,⁷⁷ pero no es hasta que la desinformación se convierte en una amenaza para los sistemas electora-

⁷⁷ Reglamento (UE) No 596/2014 del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre el abuso de mercado (Reglamento sobre abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión. <https://www.boe.es/doue/2014/173/L00001-00061.pdf>

les de los países occidentales que no comienzan a aparecer soluciones institucionales.

También se conocía la importancia que tiene el desarrollo mediático para impedir la generación de burbujas de filtro, debido a la personalización de contenidos. Debido a esto, la UE reconoció la importancia de adquirir un compromiso con el Derecho a la información y la libertad de expresión, algo básico para crear medios profesionales y confiables. Además, se observa la importancia de las plataformas en línea como elemento clave en la gobernanza electrónica, donde destaca la importancia de las decisiones tomadas por algoritmos.⁷⁸

A partir de 2015, se multiplica la aparición de informes y comunicaciones⁷⁹ de la UE sobre el uso de datos personales, plataformas en línea o noticias falsas, que converge en la aprobación de iniciativas y acciones más directas, que se han ido implementando durante 2018/2019, como el lanzamiento del Eurobarómetro en 2018⁸⁰ y la creación del grupo de expertos de alto nivel sobre la desinformación (HLEG).

78 El informe de 31 de mayo de 2017 sobre plataformas en línea y mercado único digital. http://www.europarl.europa.eu/doceo/document/A-8-2017-0204_ES.html?redirect

79 Por ejemplo, Comunicación en el marco de la estrategia para el mercado único digital de Europa, mayo 2015; advierte de la necesidad de un marco regulador <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML?uri=CELEX:52015DC0192&from=ES>. Comunicación al Parlamento europeo contra el contenido ilícito en línea; Comunicación 25 mayo 2016 sobre plataformas en línea y mercado único digital advirtiendo de la necesidad de un enfoque legal armonizado <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML?uri=CELEX:52016DC0288&from=ES>. Directiva 2016/1148 seguridad en las redes <https://www.boe.es/boe/2016/194/L00001-00030.pdf>

80 Eurobarómetro sobre *Fake News* y Desinformación en línea 2018. <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183>

En junio de 2017, el Parlamento Europeo adoptó una Resolución en la que se instaba a la Comisión a analizar el contexto y el marco jurídico existente en torno a la limitación de la difusión de noticias falsas, sopesando la posibilidad de intervenir a nivel legislativo para limitarlas. No es algo impensable que la apresurada respuesta de algunos gobiernos de la UE al fenómeno de la desinformación pueda dar lugar a daños que cristalicen en censura; para evitarlo se intentan tomar iniciativas más equilibradas a nivel supranacional que impliquen las mismas acciones en todos los Estados miembros.

En 2015 se crea el [EAST Stratcom Task Force](#) con el objetivo de frenar campañas de desinformación que, al parecer, provienen de Rusia. El [Reglamento General de Protección de Datos](#) (RGPD), aprobado en 2018, tuvo mucha influencia y creó gran expectación en cuanto a su capacidad para limitar la expansión de la desinformación. El RGPD aumentaba las posibilidades reales de protección de nuestros datos durante su tratamiento y elaboración de perfiles (considerandos 71 sobre elaboración de perfiles, artículo 17 donde se establecen condiciones para el tratamiento de datos especiales, artículo 22 posibilidad de oponerse a datos personales), lo que limitaría la transmisión directa de desinformación dirigida a determinados perfiles. Pero el Reglamento no hace referencia al *big data* o *cloud computing*, al internet de las cosas, por lo que esquivaba cuestiones fundamentales que quedan sin regular por parte del Reglamento. Realmente no se encuentra una prohibición directa, desde la UE, respecto a la elaboración de perfiles con datos personales, aunque sí se intenta limitar la recopilación y el uso de datos de manera indiscriminada y sin consentimiento.

Hay otras iniciativas plasmadas en forma de Directiva con el objetivo de que los Estados miembros puedan actuar de manera más consensuada, aunque no se trata de medidas directas creadas para limitar la desinformación. En este caso encontramos la reciente Directiva (UE) 2019/790 de Derechos de autor digital,⁸¹ que impide la reproducción de fragmentos de noticias sin permiso de los autores, lo que imposibilita la manipulación y modificación de informaciones para otros fines, o las Directivas 2011/93/UE y 2017/541 sobre contenidos ilícitos, que no frenan la desinformación pero son un soporte en la lucha contra lo que conlleva la difusión maliciosa de información.

Hasta que la UE establece el Plan de Acción de 2018, no encontramos una respuesta organizada a la desinformación a través de la coordinación de todos los Estados miembros y la cooperación con *fact checkers* independientes. La mayor acción a destacar es la puesta en marcha del Código de buenas prácticas, donde se establecen acuerdos con grandes plataformas digitales y empresas como Facebook o Google. Con el Código de buenas prácticas, algunas empresas se comprometen a limitar y controlar la desinformación, aceptando un nuevo tipo de responsabilidad. Pero, aunque las redes sociales deben colaborar en contra de la falsedad de informaciones por su responsabilidad cívica, no es su trabajo el dedicarse a la selección y diferenciación de noticias verdaderas y falsas, ya que conlleva un riesgo para el derecho de acceso a la información.

Hay varias acciones para hacer frente a la desinformación, pero es en la manipulación, uso o gestión de los datos personales de los usuarios donde está la mayor dificultad a la hora de aprobar soluciones para limitar la expansión de

81 Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE <https://www.boe.es/doue/2019/130/L00092-00125.pdf>

desinformación, pues es la llave de la persuasión política.⁸²

España, como Estado miembro de la UE, ha asumido las Directivas, Reglamentos e iniciativas contra la desinformación. Además, de manera reciente se están tomando medidas para profundizar en el tema de la desinformación. Para ello se crea la Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España.⁸³ En este documento sobre la ciberseguridad se señala, entre otras cuestiones, que ciertos actores como Estados, organizaciones terroristas o grupos de crimen organizado, así como actores individuales pueden sacar ventaja del ciberespacio con acciones de desinformación y pueden establecer ataques a instituciones o personas, e incluso se habla de guerra sobre la desinformación.

Efecto de las medidas y acciones emprendidas contra la desinformación sobre derechos fundamentales

Desde la Unión Europea, se han creado Reglamentos y Directivas que, junto con diversos informes e investigaciones sobre la difusión de desinformación, han tenido como objetivo frenar la desinformación, estableciendo marcos de actuación común a todos los países miembros. La UE se fundamenta en un conjunto de valores, libertades y derechos comunes, consignados de forma explícita en el Tratado de la Unión Europea (TUE) que suponen su fundamento político, pero el uso de las tecnologías como herramienta de comunicación ha amenazado alguno de estos valores y hay que concebir nuevas maneras de protegerlos. En general, se esperaba que la UE dispusiera una reglamentación o control más efectivo

82 <https://www.newyorker.com/tech/annals-of-technology/what-was-missing-from-mark-zuckerbergs-first-day-of-congressional-testimony>

83 http://www.congreso.es/public_oficiales/L12/CORT/BOCG/A/BOCG-12-CG-A-277.PDF

sobre el uso y venta de nuestros datos, la incidencia de *bots* y la inteligencia artificial (IA) en la difusión de información.

La utilización de tecnología genera nuevos retos desde el punto de vista del derecho: desde la violación de la privacidad hasta determinar si los datos personales que se recopilan son borrados o se utilizan para los objetivos que se plantean (Ruelas, 2019). También hay que hacer frente, desde el punto de vista social y de la regulación, a la vigilancia individual y masiva. La privacidad puede estar amenazada solo con el uso de dispositivos móviles, del correo electrónico, o simplemente por la utilización de algunos electrodomésticos.

No solo está amenazada la privacidad. De modo paradójico, la libertad de expresión se ejerce con un mayor nivel de autocensura y es una de las mayores amenazas que se ciernen sobre la profesión periodística (Méndez, L. 2015). La libertad de expresión es cada vez más una libertad de expresión vigilada, los datos son de acceso fácil, y la información clasificada de la sociedad aumenta las posibilidades de manipulación.

Aún así, no parece conveniente que los poderes públicos bloqueen los procesos de comunicación pública, ni siquiera con el objetivo de limitar la desinformación. De modo que, ante el riesgo de censura desde el ámbito privado, los poderes públicos podrían establecer condiciones a los prestadores de servicios para que garanticen el pluralismo e informen de la política en la aplicación de filtros. La existencia de controles públicos en los sistemas de autorregulación y promoción de organismos neutrales puede mantener el principio de neutralidad. Pero los esfuerzos públicos deberían centrarse en proteger el pluralismo de la red y no en el control de los contenidos (GMT Lozano, 2011), que es lo que se viene haciendo de manera general desde la UE.

No todas las medidas de la UE se incluyen dentro del marco propuesto en la lucha contra la desinformación. Por ejemplo, una de las últimas Directivas UE, la Directiva 2019/790 de Derechos de autor digital no es una medida pensada directamente para limitar la desinformación, pero

podría ayudar a limitarla. Con la aplicación de esta Directiva los editores pueden actuar como filtro de contenido para proteger los derechos de autor, pero corre el peligro de vulnerar la libertad de empresa, la privacidad o el manejo correcto de datos personales con el pretexto de proteger los derechos de autor.

Las iniciativas, regulación y medidas europeas, al igual que las que han partido desde otros países, podrían ser efectivas si actúan con el objetivo de limitar la desinformación y garantizar los derechos relacionados con la recepción y el acceso a la información. Pero existen algunas decisiones, tomadas o no de manera consciente por gobiernos u organizaciones, que pueden limitar libertad de expresión u otros derechos. Es por esto que, el 7 de marzo de 2017 la Organización para la seguridad y cooperación en Europa (OSCE) junto a la Organización de Naciones Unidas (ONU), la Comisión Interamericana de Derechos Humanos (CIDH), la Organización de Estados Americanos (OEA) y la Comisión Africana de Derechos Humanos, emite una Declaración donde advierte sobre iniciativas pensadas para frenar la desinformación realizadas desde el sector público y privado, que intentan limitar la libertad de expresión, circulación de ideas o el disenso, iniciativas contrarias al derecho internacional de los derechos humanos. En esta Declaración se advierte, entre otras cosas, que el bloqueo de IP o sitios web, solo puede realizarse si lo estipula la ley, protegiendo los derechos humanos; los sistemas de filtrado no los pueden controlar los gobiernos debido a que pueden restringir libertad de expresión. No se debe prohibir la desinformación con conceptos imprecisos, e instan a promover alfabetización y los medios veraces independientes.

Relación entre derechos fundamentales y control de la desinformación: el caso de España

La pertenencia a la UE no garantiza que Estados miem-

bros pongan en marcha iniciativas legislativas para controlar la desinformación o el ciberespacio y que no supongan riesgo para el ejercicio de derechos fundamentales. El caso de España puede servir para mostrar que la elaboración de normativa nacional para limitar la desinformación o regular las redes, puede incurrir en la adopción de medidas que afecten a derechos fundamentales, a pesar de la normativa impuesta desde Bruselas.

España adecúa a su marco jurídico la normativa promulgada por la UE, y aunque generalmente la normativa de carácter obligatorio es extensible a todos los países miembros, se comprueba que pueden existir leyes discordantes con algunas de las Directivas, o simplemente pueden llegar a ser incompatibles con la protección y el ejercicio de otros derechos.

En noviembre de 2018 se aprobó en España el artículo 58 bis, modificando la Ley orgánica del Régimen electoral General (LOREG) que autorizaba a los partidos a recopilar datos de las personas para el envío de propaganda electoral por redes o a través de internet, realizando perfiles ideológicos. De este modo, se permitía a partidos políticos a rastrear datos personales y opiniones políticas, de páginas web o redes sociales, para elaborar perfiles, permitiendo el llamado *spam* electoral, medida totalmente contraria al RGPD que recién entraba en vigor en mayo de ese mismo año. Para evitar la aprobación de este artículo, se puso en marcha un recurso de inconstitucionalidad, admitido a trámite este mes de marzo por el Tribunal Constitucional.⁸⁴ Finalmente, este artículo ha sido anulado por el mismo Tribunal. La puesta en marcha de esta ley se apoyaba en el considerando 56 del RGPD,⁸⁵ que fue utilizado para legitimar este sistema de elaboración de perfiles.

En España existe una comisión sobre noticias falsas que depende, desde 2018, de la Comisión de Seguridad Nacio-

84 <https://www.boe.es/boe/dias/2019/03/15/pdfs/BOE-A-2019-3698.pdf>

85 <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

nal. Y es, según la estrategia de Seguridad Nacional que se aprueba el 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. Según el texto de la ley, la normativa se adapta a las nuevas tecnologías y redes de comunicaciones por parte de las Administraciones Públicas y garantiza el interés general y la seguridad pública, avalado por la Ley 36/2015 de Seguridad Nacional, que describe riesgos asociados a nuevas tecnologías.

El Real Decreto hace referencia a los desafíos que plantean las redes, como la desinformación, las interferencias en procesos de participación política de la ciudadanía y espionaje, por lo que se modifica el marco legislativo para hacer frente a la situación con medidas urgentes relativas a los datos que poseen las administraciones públicas. Establece medidas para reforzar la coordinación en materia de seguridad de las redes y sistemas de información, reforzando la normativa sobre protección de datos personales y la protección de la seguridad pública en este ámbito.

Los análisis realizados sobre este Real Decreto coinciden en que su intención es, entre otras cosas, proteger contra el robo de datos y sobre todo prevenir la creación de una administración digital paralela. Según Rights International,⁸⁶ en este Real Decreto se realizan referencias abstractas, sin mencionar que se atribuye a la Administración del Estado una serie de competencias amplias con vocación de permanencia, que afectan derechos de los ciudadanos. Lo más polémico de este Real Decreto es que, mediante la modificación de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, puede dar lugar a la posibilidad de cierre de webs sin autorización judicial, en supuestos excepcionales que atenten al orden o la seguridad pública o nacional. Pero no se puede proceder

86 <http://www.rightsinternationalspain.org/es/blog/157/censura-digital-cuando-se-puede-cerrar-una-web-por-decreto>

al cierre de ninguna página a no ser que se haya cometido un delito, por lo que hay posibilidades de que suceda, como en la ley del *spam* político, que acabe en el Constitucional.

Según Civio, ya estaba permitido ordenar el cese de urgencia de una página, y sin audiencia previa de forma cautelar, por razones de seguridad pública, protección civil, emergencias, defensa de la vida humana o interferencia con otras redes. Pero ahora las razones son mucho más amplias: la facultad de intervenir servicios o redes podrá afectar a “cualquier infraestructura, recurso asociado o elemento o nivel de la red”. No hace referencia solo al cierre de webs, sino de cualquier elemento de las comunicaciones digitales, también estructurales, como el corte de la conexión, por ejemplo. El Gobierno ha aprovechado este Decreto Ley para añadir otra justificación al cierre exprés de páginas web u otros servicios de comunicaciones digitales: “Cuando cree graves problemas económicos u operativos a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas o demás usuarios del espectro radioeléctrico”, y veta el *blockchain* hasta que la UE regule si se puede usar este sistema en las Administraciones Públicas.⁸⁷

Conclusión

La mayor fortaleza de la desinformación y la mayor amenaza a la libertad y derechos ciudadanos provienen de la capacidad de acumular informaciones personales, por lo que la regulación debería promover tecnologías que garanticen la privacidad, sobre todo en redes sociales. La implicación e

87 <https://civio.es/el-boe-nuestro-de-cada-dia/2019/11/05/las-administraciones-publicas-tienen-seis-meses-para-que-todas-sus-bases-y-servicios-con-datos-personales-estén-alojadas-en-servidores-europeos/>

importancia de redes sociales en la desinformación es básica, lo señala incluso el informe del Centro de comunicaciones estratégicas de la Organización del Tratado del Atlántico Norte (OTAN)⁸⁸ realizado este año, en el que se advierte de la laxitud de las redes sociales en la lucha contra la desinformación; es más, la lucha contra la desinformación de manera coordinada está lejos de terminar. Las grandes empresas podrían impedir la difusión de desinformación explicando cómo funcionan los algoritmos y seleccionan las noticias, mediante la transparencia. La legislación podría basarse en definiciones más precisas con el objetivo de hacer frente a las causas de desinformación, garantizando el proceso legal, la proporcionalidad y responsabilidad, antes que dejar toda la responsabilidad a las empresas privadas, aunque también la tengan, con el riesgo que eso conlleva.

Pero, incluso conscientes de que existe desinformación, prohibir de manera específica la difusión supone un riesgo. Es posible y necesario equilibrar la libertad de expresión, la privacidad y el derecho a estar bien informado.

Las iniciativas para contrarrestar la desinformación sin limitar otros derechos pasan por promover servicios de filtrado de noticias, una mejora de la transparencia en la distribución de noticias *online* o promover la alfabetización mediática, empoderando a los usuarios, ya que la participación, a veces inconsciente, del usuario es fundamental en la difusión de desinformación.

A pesar de todas estas medidas hay nuevos problemas asociados a la desinformación que van a ser muy difíciles de controlar, como la microsegmentación. Es una actividad centrada en la recopilación abusiva de datos personales que se transmiten hacia otras web o servicios digitales. Combinando toda la información se diferencia a los usuarios. Con esta técnica ni siquiera da resultado camuflar la huella digital. La mi-

88 <https://www.stratcomcoe.org/how-social-media-companies-are-failing-combat-inauthentic-behaviour-online>

crosegmentación puede vulnerar derechos humanos como la dignidad humana o los derechos a la autonomía y privacidad.

En general, parece que las medidas para frenar la desinformación son siempre insuficientes debido a la rapidez, los cambios en la comunicación y sus herramientas. Pero no se debería utilizar cualquier instrumento para controlar la desinformación, ya que puede ser utilizado para prescindir de alguno de nuestros derechos fundamentales sobre los que hay que reforzar la protección.

Bibliografía

- Chulvi, C. P. (2018). Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red. *Teoría y Realidad Constitucional*, (41), 297-318.
- Galdámez Morales, Ana. "Posverdad y crisis de legitimidad". [Revista española de la transparencia](#), ISSN-e 2444-2607, [N.º. 8, 2019](#) (Ejemplar dedicado a: Revista Española de la Transparencia número 8 (primer semestre 2019), pp. 25-44.
- Germán M. Teruel Lozano. "Libertad de expresión en Internet, control de contenidos de las páginas web y sus garantías constitucionales". *Revista Aranzadi de derecho y nuevas tecnologías*, ISSN 1696-0351, N.º. 25, 2011, pp. 81-103.
- Méndez, L. (2015). Certezas sobre el estado de la libertad de prensa en España. *Cuadernos de periodistas: revista de la Asociación de la Prensa de Madrid*, (30), 12-20.
- Merlos, A. (2018). Políticas de seguridad y defensa en la era de la posverdad. *Cuadernos de estrategia*, (197), 83-106.
- Ruelas Monjardín, A. (2019). "Metodología Jurídica Digital: conceptualización y problemáticas para su construcción". 01/01/2019. *Derecho y Cambio Social*. N.º 55 enero-marzo 2019 (pp.1-36)

Documentos UE

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Reglamento (UE) No 596/2014 del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre el abuso de mercado (Reglamento sobre abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión <https://www.boe.es/doue/2014/173/L00001-00061.pdf>

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016. Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. <https://www.boe.es/doue/2016/194/L00001-00030.pdf>

Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE <https://www.boe.es/doue/2019/130/L00092-00125.pdf>

Comunicación en el marco de la estrategia para el mercado único digital de Europa, mayo 2015. <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0192&from=ES>

Comunicación 25 mayo 2016. Las plataformas en línea y el mercado único digital Retos y oportunidades para Europa. <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52016DC0288&from=ES>.

Informe de 31 de mayo de 2017 sobre plataformas en línea y mercado único digital. http://www.europarl.europa.eu/doceo/document/A-8-2017-0204_ES.html?redirect

- A multi-dimensional approach to disinformation. 2108. Report of the independent High Level Group (HLEG) on fake news and online disinformation. Informe del grupo de expertos de alto nivel de la Unión Europea. <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>
- Código de Buenas Prácticas. Code of Practice on Disinformation. <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>
- Eurobarómetro 2018. “Fake news and Disinformation Online”. Febrero/marzo 2018. <https://ec.europa.eu/comm-frontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183>

Otras publicaciones

- Recurso de inconstitucionalidad n.º 1405-2019, contra el artículo 58 bis.1 de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, incorporado a esta por la disposición final tercera, punto dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. <https://www.boe.es/boe/dias/2019/03/15/pdfs/BOE-A-2019-3698.pdf>
- World Economic Forum (2019). Global Risk 2019. Recuperado de: http://reports.weforum.org/global-risks-2019/chapter-one/?doing_wp_cron=1576673713.0500071048736572265625
- Del Castillo, Carlos (2 de febrero 2019). “Hasta el más pequeño detalle se usa para saber quién eres: así es la huella digital que dejas en Internet”. *ElDiario.es*. Recuperado de: https://www.eldiario.es/tecnologia/funciona-digital-millonnes-ordenadores-smartphones_0_865463781.html; <https://www.aepd.es/media/estudios/estudio-fingerprinting-huella-digital.pdf>

Chen, Adrian. (11 de abril 2018). *The New Yorker*. Recuperado de:

<https://www.newyorker.com/tech/annals-of-technology/what-was-missing-from-mark-zuckerbergs-first-day-of-congressional-testimony>

Belmonte, Eva (11 de mayo 2019). *Civio*. Recuperado de:

<https://civio.es/el-boe-nuestro-de-cada-dia/2019/11/05/las-administraciones-publicas-tienen-seis-meses-para-que-todas-sus-bases-y-servicios-con-datos-personales-estén-alojadas-en-servidores-europeos/>

OTAN (2019). How Social Media Companies are Failing to Combat Inauthentic Behaviour Online. Platforms. Report from NATO StratCom COE. Recuperado de: https://www.reddit.com/.../e6zo6m/how_social_media_companies_are_failing_to_combat

[Rights International Spain \(2019\)](http://www.rights-internationalspain.org/es/blog/157/censura-digital-cuando-se-puede-cerrar-una-web-por-decreto). Censura digital, cuando se puede cerrar una web por Decreto. <http://www.rights-internationalspain.org/es/blog/157/censura-digital-cuando-se-puede-cerrar-una-web-por-decreto>