QUIÉN, CÓMO Y QUÉ REGULAR (O NO REGULAR) FRENTE A LA DESINFORMACIÓN

LORENZO COTINO HUESO[1]
Catedrático de Derecho Constitucional
Universidad de Valencia

TRC, n.º 49, 2022, pp. 199-238
ISSN 1139-5583

SUMARIO

I. LOS CONCEPTOS NORMATIVOS —Y LA REGULACIÓN— DEJAN SIN ABORDAR MUCHOS FENÓMENOS DE DESINFORMACIÓN

El fenómeno que aquí ocupa se intenta encapsular con diversa terminología. La más general serían los «desórdenes informativos» (*information disorder*), entre

1 Investigador de la Universidad Católica de Colombia. Coordinador del Grupo de Trabajo Legal del Grupo de Expertos en la lucha contra la desinformación, Departamento de Seguridad Nacional, 2021-2022. En cualquier caso, el presente documento sólo expresa las posiciones del autor. El estudio es resultado de investigación del proyecto «Derecho, Cambio Climático y Big Data», Universidad Católica de Colombia. De igual modo, realizado en el marco de los proyectos MICINN Retos «Derechos y garantías frente a las decisiones automatizadas...» (RTI2018-097172-B-C21); «La regulación de la transformación digital y la economía colaborativa» Prometeo/2017/064 Generalitat Valenciana, 2017-2021 y «Algoritmic law» (Prometeo/2021/009, 2021-24).

los que estaría la información errónea pero sin ánimo de dañar (*mis-information*), la desinformación con ánimo de hacer daño *(dis-information,*) y mala información (*mal-information)*, cuando se revela información cierta pero privada para hacer daño. El fenómeno se describe también con expresiones de polución informativa, postverdad, notificas falsas o *fake news*, comportamiento inauténtico coordinado o propaganda computacional, así como en términos de operaciones de influencia indebida, desinformación estructurada, guerra cognitiva y otras.

La noción de «desinformación» presenta algunos consensos, como «información falsa y creada deliberadamente para perjudicar a una persona, grupo social, organización o país»[2] que se ha empleado por el Grupo de expertos de alto nivel de la UE[3]. El Plan de Acción contra la desinformación de 12 de diciembre de 2018[4], en la misma línea, hace referencia a la «intención de engañar o de obtener una ganancia económica o política y que puede causar un perjuicio público»[5]. Desde distintos ámbitos —como por ejemplo las plataformas y redes—, en vez de fijar la atención en si los contenidos son desinformación desinformativos, se subrayan los elementos descriptivos de la conducta y el comportamiento de los sujetos que desinforman a través de las nuevas tecnologías. Así, objetivar el concepto, hacerlo más técnico e incluso aséptico, de este modo se mitiga el siempre sensible juicio de la falsedad del contenido de la información.

Hay que estar prevenido frente a quien afirme que hay un concepto objetivo de desinformación ajeno a la política y, sobre todo, inmune al peligro de afectar a los derechos fundamentales y principios constitucionales en la lucha contra la misma. Por lo que aquí interesa, jurídica y normativamente es esencial partir de un concepto delimitado y restrictivo desinformación por cuanto a las implicaciones concretas que pueden derivar, más si cabe si de lo que se trata es de una respuesta penal o sancionadora. Como consecuencia de estos conceptos restrictivos, ya se puede adelantar que, al menos en los países que cumplen los estándares democráticos, los conceptos de desinformación que se manejan normativamente dejan fuera muchas realidades que comúnmente se identifican como desinformación. Es por ello que jurídicamente hay que asumir que muchos fenómenos desinformativos no pueden tener respuesta legal alguna en los países democráticos. La acción pública en todo caso es muy importante como en el terreno de la educación

2 Consejo de Europa-Wardle, C. y Derakhshan, H., *Information Disorder: Toward an interdisciplinary framework for research and policymaking*, Consejo de Europa, 2017, Estrasburgo, p. 6 y p. 20 https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

3 HLG-UE, *Informe final A multidimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation*. Directorate-General for Communication Networks, Content and Technology, 12 de marzo de 2018, https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation

4 Consejo de la UE. *Plan de Acción contra la desinformación*, Bruselas, 12 de diciembre de 2018 https://data.consilium.europa.eu/doc/document/ST-15431-2018-INIT/es/pdf

5 Comisión Europea, *Comunicación COM(2020) 790 final, sobre el Plan de Acción para la Democracia Europea,* Bruselas, 3.12.2020, p. 7, apartado 4.º https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0790&from=ES

y la alfabetización mediática. Es esencial la programación de la enseñanza y la adaptación curricular, la capacitación docente, generar conciencia, pensamiento crítico, sensibilización y capacitación para detectar y reaccionar frente a la desinformación. No obstante, no es el objeto de atención de este estudio.

Volviendo a los conceptos normativos, resulta útil recordar algunas delimitaciones legislativas del concepto en países democráticos. Previamente al fenómeno digital, cabe destacar varias leyes 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.»[6] 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 la jurisprudencia ha sido muy restrictiva y son muy extrañas las condenas por aplicación de estos preceptos[7].

Ya para el fenómeno de la desinformación en el mundo digital, hay que destacar la Ley n.º 2018-1202 de 22 de diciembre de 2018 de lucha contra la manipulación de información[8]. 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 sinceridad 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 n.º 2018-773 DC de 20 de diciembre de 2018[9] al interpretar esta ley exige garantías en claro sentido restrictivo, 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 sinceridad de la votación». Según lo adelantado, estos elementos interpretativos conceptuales son un buen punto de partida desde el punto de vista jurídico para determinar sobre qué tipo de desinformación puede actuarse. Y eso que no se trata de una ley sancionadora o penal que habría de interpretarse de modo aún más restrictivo.

6 https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000877119/

7 https://www.legavox.fr/blog/maitre-anthony-bem/repression-fausses-nouvelles-fake-news-24479.htm

8 https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559#:~:text=%2DLe%20Conseil%20sup%C3%A9rieur%20de%20l,1%20de%20la%20pr%C3%A9sente%20loi.

9 https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847711/

En Canadá, la *Elections Modernization Act*, de 13 de diciembrte de 2018 (Bill C-76, art. 282. 4, 1)[10] prohíbe en general la «Influencia indebida por parte de extranjeros» para las votaciones y gastos. Este concepto también sería muy amplio para establecer una prohibición general, de ahí que debe advertirse que la ley incluye excepciones muy amplias, de modo que se permite a extranjeros opinar o hacer reportajes a favor de unos resultados o a favor de candidatos.

En la reciente propuesta legislativa de Reino Unido de 12 de mayo de 2021 (*Online Safety Bill*)[11] se 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 alcance de las medidas contra la desinformación, el Comité de la Cámara de los Lores ya ha insistido en que los «daños» han de ser a personas físicas «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.»[12].

Si en los sistemas democráticos el concepto de desinformación queda severamente restringido, todo lo contrario sucede en los países que no cumplen o sólo relativamente los estándares democráticos. Los Relatores internacionales para la libertad de expresión en su Declaración conjunta de marzo de 2017 pronto afirmaron que «Las prohibiciones generales de difusión de información basadas en conceptos imprecisos y ambiguos, incluidos «noticias falsas» («fake news») o «información no objetiva», son incompatibles con los estándares internacionales sobre restricciones a la libertad de expresión, [...] y deberían ser derogadas.»[13]

Siguiendo alguna base de datos de la regulación de la desinformación[14] o algunos estudios de regulación comparada[15] pueden encontrarse leyes o proyectos legislativos que criminalizan, por ejemplo, difundir «propaganda» o el contenido «agresivo y aterrador» (Bangladesh); difundir información falsa en línea (Bielorrusia), o contenidos que «amenazan la seguridad nacional» (Camboya). También se criminaliza informar de «cualquier noticia sin poder demostrar su verdad o que se tiene una buena razón para creer que es verdad» (Camerún); «difundir información falsa a sabiendas» (Kazajstán o Kenia); «noticias falsas»

10 https://www.parl.ca/DocumentViewer/en/42-1/bill/C-76/royal-assent

11 https://www.gov.uk/government/publications/draft-online-safety-bill

12 Woodhouse, J., *Regulating online harms*, House of Commons Library, Londres, 12 agosto 2021, p. 33 https://commonslibrary.parliament.uk/research-briefings/cbp-8743/

13 Relatores internacionales para la libertad de expresión, *Declaración Conjunta Sobre Libertad De Expresión y «Noticias Falsas» («Fake News»), Desinformación y Propaganda*, marzo 2017, Punto 2. a) http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1056&lID=2

14 Funke, D. and Flamini, D., *A guide to anti-misinformation actions around the world,* Poynter, 2018, https://www.poynter.org/ifcn/anti-misinformation-actions/

15 Law Library of Congress US, *Initiatives to counter fake news in selected countries*, Washington, D.C.: Law Library of Congress US, 2019, https://www.loc.gov/item/2019668145/ y, también, *Government responses to disinformation on social media platforms*, Washington, https://www.loc.gov/item/2019713404/

(*fake news*) en Egipto; la publicación de «información incorrecta» que cause «temor o alarma al público» (Myanmar), «cualquier noticia, información, datos e informes que sean total o parcialmente falsos, ya sea en forma de características, imágenes o grabaciones de audio o en cualquier otra forma capaz de sugerir palabras o ideas» (Malasia).

Otro ejemplo destacable para no seguir es el de Rusia. La Ley Federal del 18 de marzo de 2019 N 30-ФЗ de «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»[16]. 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» (art. 10). Y sólo unos días después de la invasión de Ucrania, al parecer el 4 de marzo se ha pasado a castigar con 15 años de prisión las «noticias falsas» sobre el ejército ruso. Y ello se acompaña con la Ley Federal del 1 de mayo de 2019 N 90-ФЗ[17], 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 y «contrarestar amenazas» si declara que hay una situación de emergencia en razón de una campaña de desinformación (art. 65). Como luego se comenta, se trata de un modelo de soberanía de Internet rechazado desde Occidente. Estas normas se han aplicado contundentemente desde el inicio de la invasión para anular las principales plataformas.

II. PRESUPUESTOS REGULATORIOS DESDE LAS LIBERTADES INFORMATIVAS

Desde el Consejo de Europa se ha analizado el alcance de la libertad de expresión en Internet[18] y la Comisión de Venecia[19] establece como punto de partida la especial protección de la libertad de expresión en periodo electoral, así como la necesidad mantener un Internet abierto y neutral en elecciones (principio n.º 2). La muy amplia e intensa protección de la libertad de expresión e información por la jurisprudencia europea y española hace que sea especialmente sensible y difícil cualquier regulación de la desinformación[20].

16 http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264

17 https://rg.ru/2019/05/07/fz90-dok.html

18 Consejo de Europa, *Internet: case-law of the European Court of Human Rights*, junio 2015, www.echr.coe.int/documents/research_report_internet_eng.pdf

19 Comisión de Venecia, *Opinión 974/2019, de 11 de diciembre de 2020, Principles for a fundamental rights-compliant use of digital technologies in electoral processes*, Estrasburgo, diciembre 2020, principio n.º 1 https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2020)037-e

20 Especialmente cabe seguir Pauner Chulvi, C., «Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la Red». *Teoría y Realidad Constitucional*, n.º 41, 2018,

Cabe señalar algunos presupuestos en la materia. Bien es cierto que las libertades informativas no alcanzan a proteger en Europa un derecho a mentir. Se llega a afirmar que no existe el derecho a no recibir información manipulada o tendenciosa, a no ser víctima de la desinformación[21], o que el mensaje sea o no verdadero es irrelevante para su protección constitucional[22]. La Constitución protege la información que es veraz. No obstante, hay que partir de que la veracidad sólo se predica de la información y los hechos, no de la opinión. Así, se imposibilita el control de la verdad o mentira cuando se trata de opiniones. Asimismo, se dificulta mucho el control de la veracidad de informaciones en cuanto están impregnadas de la libertad de expresión, lo cual es extraordinariamente fácil. El Tribunal Constitucional español (STC 214/1991) 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 contrarias a la dignidad humana). Asimismo, ha señalado que «las afirmaciones erróneas son inevitables en un debate libre, de tal forma que de imponerse la «verdad» como condición para el reconocimiento del derecho, la única garantía de la seguridad jurídica sería el silencio» (STC 6/1988). Debe recordarse igualmente que la libertad de expresión sí que protege muchas formas de interpretar los hechos en una sociedad democrática (STEDH, Handyside v. Reino Unido 1976). La STEDH Růžový panter, o.s. v. República Checa, de 2 de febrero de 2012 afirmó que «La distorsión de la verdad, de mala fe, a veces puede sobrepasar los límites de una crítica aceptable: una declaración verdadera puede ir acompañada de comentarios adicionales, juicios de valor, suposiciones e incluso insinuaciones que podrían dar al público una imagen equivocada». (§ 32). «La información debe tener suficiente base factual —coincidencia con el referente externo—, sin lo cual sería excesiva.» (STEDH de 27 de febrero de 2001, caso Jerusalén contra Austria, § 43). La más reciente STC 8/2022, de 27 de enero aborda de pleno las libertades informativas en las redes sociales, eso sí, con escasas soluciones. Respecto de quienes generan la desinformación, y especialmente para los profesionales de la desinformación, el TC afirma que imponerles una sanción civil implica «un mensaje dirigido a la totalidad de

pp. 297-318. https://doi.org/10.5944/trc.41.2018.22123ba; Catoira, A. (2020). «Los desórdenes informativos en un sistema de comunicación democrático». *Revista de Derecho Político*, n.º 109, septiembre-diciembre 2020, pp. 119-151 https://doi.org/10.5944/rdp.109.2020.29056. También, Garrigues Walker, A. y González de la Garza, L. M. *El Derecho a no ser engañado. Y cómo nos engañan y nos autoengañamos*, Thomson Reuters Aranzadi, 2021.

21 Al momento de cerrar este estudio, la mejor aproximación sin duda la de Serra Cristóbal, R., «De falsedades, mentiras y otras técnicas que faltan a la verdad para influir en la opinión pública», *Teoría y Realidad Constitucional*, n.º 47, 2021, pp. 199-235, cita p. 231 https://doi.org/10.5944/trc.47.2021.30712.

22 Afirmación de Villaverde Menéndez, I., «Verdad y constitución. Una incipiente dogmática de las ficciones constitucionales», *Revista Española de Derecho Constitucional,* n.º 106, pp. 149-201, p. 149, http://dx.doi.org/10.18042/cepc/redc.106.04

los usuarios de que la publicación de informaciones falsas en internet, más concretamente en redes sociales, y en particular por parte de profesionales de la comunicación, es una falta de atención de los deberes y responsabilidades que les vinculan» (FJ 4º). Habrá que ver hacia dónde deriva este tipo de afirmaciones.

Ahora bien, no hay que olvidar que el ejercicio de la libertad de expresión y de información está más intensamente protegido cuando se vincula a cuestiones de interés general o cuestiones políticas y especialmente en periodo electoral (Mouvement raëlien Suisse v. Suiza de 13 de julio 2012). De ahí que las posibilidades de restringirlas son menores y las exageraciones y afirmaciones desmedidas están más protegidas (STEDH Willem c. Francia, 16 de julio de 2009, § 33). En el ámbito político, que es precisamente dónde más incide la desinformación, se protegen las exageraciones (STEDH, Renaud v. Francia, de 25 de febrero de 2010) y no hay que probar la verdad de los juicios críticos (Dalban v. Rumania, de 28 de septiembre de 1999). En esta dirección, más recientemente la STEDH de 25 de julio de 2019 (Asunto Brzezinski contra Polonia) consideró violación de la libertad de expresión que, siguiendo la ley electoral polaca, un juez prohibiese la distribución de un folleto electoral que incluía información falsa.

Debe advertirse también que en general las medidas que se adopten contra la desinformación no pueden ampararse en la prohibición de abuso de derecho del artículo 17 CEDH y 54 de la Carta de Derechos fundamentales de la UE. Considero que la jurisprudencia actual difícilmente legitima restricciones generales por abuso de derecho basadas en la calidad de la información[23].

De los anteriores lineamientos lo que sin ninguna duda puede desprenderse es que la evaluación de la falsedad de contenidos emitidos en el contexto político es una cuestión muy compleja y sensible desde la libertad de expresión y de información. De ahí que haya que extremar las cautelas, especialmente respecto de quiénes pueden hacer la evaluación de la falsedad de contenidos. Como se verá, esta evaluación es extraordinariamente peligrosa en manos del Gobierno, de autoridades no independientes, incluso de las que así se califican. Presenta también muchos problemas que el control lo efectúen las plataformas o redes, incluso los llamados verificadores. En muy buena medida, en la lucha contra la desinformación el remedio es peor que la enfermedad, lo cual obliga a puntos de partida de acción muy concretos y posibilistas.

1. **En muchos ámbitos lo mejor es no regular**

Debe evitarse una criminalización general de la desinformación, esto es, la regulación de conductas sancionables penal o administrativamente, en especial

23 Ver STEDH Pavel Ivanov contra Rusia, de 20 de febrero de 2007; STEDH Féret contra Bélgica, de 16 de julio de 2009; STEDH Norwood contra Reino Unido, de 16 de noviembre de 2004.

expresiones y conceptos generales que se han mencionado. Como señala la relatora de libertad de expresión en 2021 «El derecho penal solo debería utilizarse en circunstancias muy excepcionales y graves de incitación a la violencia, el odio o la discriminación.»[24].

Cuestión diferente es que algunas manifestaciones más concretas de la desinformación sí puedan ser objeto de regulación o ya estén tipificadas como delito en la legislación vigente. Así, si se sigue a nuestra Fiscalía General del Estado[25], esto podría suceder con los delitos de odio, revelación de secretos, delitos contra la integridad moral, desórdenes públicos, injurias y calumnias, contra la salud pública, estafas, intrusismo o delitos contra el mercado y los consumidores. Habrá que analizar cada conducta concreta y su encaje en estos delitos y no bajo la persecución de la desinformación en sí. Y en todo caso, debe recordarse la interpretación restrictiva que siempre opera en el Derecho penal y sancionador. Asimismo, hay que tener en cuenta la especial conflictividad de algunos de estos delitos, como en particular los delitos de odio (art. 510 Código Penal) que en cualquier caso deben interpretarse bajo la libertad de expresión[26].

2. **Hay que evitar que órganos gubernamentales no independientes evalúen los contenidos, ponderen derechos y puedan orquestar debate político**

Debe huirse de los sistemas que permitan que órganos gubernamentales evalúen la veracidad de los contenidos y que ponderen la libertad de expresión e información con otros derechos o bienes. Se considera un acertado punto de partida el general de Estados Unidos[27]. Allí se huye de cualquier valoración de contenidos por las autoridades que pueda suponer orquestar el debate político. La «Counterspeech Doctrine» establecida por el juez Brandeis (caso Whitney v. California, 1927) viene a suponer que frente a «las falsedades y falacias [...] el remedio a aplicar es más discurso, no el silencio forzado», esto es, más deliberación y libertad de expresión. Así lo expresa en 2012 el juez Kennedy en Estados

24 Relatora de libertad de expresión, *Infome al Consejo de Derechos Humanos, «La desinformación y la libertad de opinión y de expresión»,* ONU, 13 de abril 2021, n.º 89. https://undocs.org/es/A/HRC/47/25

25 Fiscalía General del Estado, *Tratamiento penal de las «Fake news»*, 2020, https://www.icab.es/export/sites/icab/.galleries/documents-noticies/tratamiento-penal-de-las-fake-news-fiscalia-general-del-estado.pdf

26 Sobre el tema, cabe remitir a LIBEX, *Incitación al odio, la violencia o la discriminación contra grupos vulnerables*, 2021, https://libex.es/incitacion-odio-violencia-discriminacion-vulnerables/; Teruel Lozano, G. M., «Cuando las palabras generan odio: límites a la libertad de expresión en el ordenamiento constitucional español», Revista española de derecho constitucional, Año n.º 38, n.º 114, 2018, pp. 13-45, doi: https://doi.org/10.18042/cepc/redc114.01 o Rollnert Liern, G. «Redes sociales y discurso del odio: perspectiva internacional». *IDP: revista de Internet, derecho y política*, n.º 31, UOC, 2020, pp. 1-14. http://dx.doi.org/10.7238/idp.v0i31.3233

27 PEN America, *Faking News. Fraudulent News and the Fight for Truth*, octubre, 2017, p. 20, https://pen.org/research-resources/faking-news/

Unidos. v. Álvarez[28]: «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». Como señala el juez Kozinksi en esta decisión tan importante. «Si todo discurso falso está desprotegido {por la libertad de expresión…} tendríamos que censurar nuestro discurso para evitar el riesgo de enjuiciamiento por decir algo que resulta falso. La Primera Enmienda no tolera darle al Gobierno tal poder».

Como más adelante se señala, en el futuro pueden cobrar una gran relevancia los «coordinadores de servicios digitales» de los que habla la propuesta de *Digital Services Act* de la UE (DSA, «ley de servicios digitales»), que pueden incidir directa o indirectamente en los contenidos que finalmente son accesibles a los usuarios de plataformas y redes sociales o resolver reclamaciones de los usuarios frente a las acciones de las plataformas o decidir qué órganos de resolución de conflictos o alertadores están capacitados para tomar decisiones sobre los contenidos, entre otros. El proyecto de ley en Reino Unido de 12 de mayo de 2021 también concede muy importantes potestades al órgano regulador, el Ofcom.

Diferentes expresiones del fenómeno de la desinformación también pueden acabar ante decisiones de autoridades estatales diversas en razón de su competencia (consumo, protección de la mujer, del menor, protección de datos, competencia, memoria democrática, etc.). Incluso en el ámbito de acciones de carácter sancionador o que, en cualquier caso, impliquen la evaluación de derechos y, finalmente una restricción o bloqueo de contenidos.

Pues bien, dada la grave sensibilidad constitucional y complejidad de la cuestión hay que ser especialmente cautelosos. En Francia y respecto de Internet, el Consejo Constitucional ha considerado inconstitucional la intervención administrativa no judicial para impedir el acceso a Internet[29] o para declarar la ilegalidad de contenidos en línea[30]. Como principio, si alguna autoridad ha de llevar a cabo estas evaluaciones con posibles consecuencias restrictivas debe ser de naturaleza judicial o gozar de un carácter indiscutiblemente independiente y neutral. Por su trayectoria, naturaleza y composición la Junta Electoral a mi juicio no presenta dudas en el ámbito de sus competencias. Sin embargo, quien suscribe considera inadecuado reconocer estas facultades a órganos reguladores del ámbito del audiovisual. Bien es cierto que la STC 86/2017, de 4 de julio

28 https://www.ca9.uscourts.gov/datastore/opinions/2011/03/21/08-50345.pdf

29 *Decisión n.º 2009-580 de 10 de junio sobre la ley HADOPI I,* 2009, n.º 14, https://www.conseil-constitutionnel.fr/es/decision/2009/2009580DC.htm

30 *Decisión n ° 2020-801 DC de 18 de junio sobre la Ley para combatir el contenido que incita al odio en Internet*, 2020, n.º 7, https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm

(FJ 5.º) consideró constitucional que el Consell de l'Audiovisual de Catalunya — CAC (autoridad según su regulación, independiente) pueda adoptar por urgencia medidas cautelares o sanciones que implican el cese provisional o definitivo de la actividad audiovisual, que contaban con base legal (art. 116 de la Ley 22/2005) y por cuanto eran recurribles judicialmente. No obstante, se trata de una sentencia más que cuestionable[31] que sería deseable que fuera matizada en futuras decisiones. En cualquier caso, debe garantizarse que estas autoridades no judiciales sean auténticamente independientes. Me atrevo a apuntar que, de tratarse de órganos colegiados, en su composición, debe garantizarse 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.

III. LA COMPLETA RESPUESTA A LA DESINFORMACIÓN DESDE LA UE, SU CÓDIGO DE BUENAS PRÁCTICAS Y EL ESPACIO A LA REGULACIÓN NACIONAL

Especialmente tras el referéndum del *Brexit* de 2016 y diversas acciones atribuidas a Rusia, han sido muchas las acciones de la UE en materia de desinformación. La preocupación se materializó en la constitución de un grupo de expertos de alto nivel y su Informe Final de 12 de marzo de 2018[32]. Ahí se establecieron las líneas maestras del modelo de la UE frente a la desinformación: fortalecer el ecosistema mediático, a los medios, periodistas y usuarios; la transparencia de las noticias; la investigación de la cuestión. Asimismo, se subrayó el peso de las plataformas y sus esfuerzos en identificar y eliminar cuentas, así como la inclusión de contenidos fiables y alternativos y la colaboración con *fact checkers* independientes. La Recomendación (UE) 2018/334, de 1 de marzo[33] sobre medidas para combatir eficazmente los contenidos ilícitos en línea aborda la desinformación en el marco de la responsabilidad de prestadores, si bien con la advertencia de que

31 Al respecto, Doménech, G., «La policía administrativa de la libertad de expresión (y su disconformidad con la Constitución)», en Efrén Ríos, L. y Spigno, I. (eds.). *La libertad de expresión en el siglo xxi. Cuestiones actuales y problemáticas*, Tirant Lo Blanch, México, 2021, pp. 193-215., se sigue https://www.academia.edu/38391193/La_policia_administrativa_de_la_libertad_de_expresion_y_su_disconformidad_con_la_Constitucion_ También, Martínez Otero, J. M., «Policía administrativa, discurso del odio y explosiones en cervecerías alemanas. A propósito de la Resolución Sancionadora 87/2018 de la CNMC, en la que se multa a Libertad Digital por incitar al oido contra los ciudadanos alemanes», *Revista General de Derecho Administrativo*, n.º 51, 2019. Ver también, Cotino Hueso, L. «ONLINE-OFFLINE. Las garantías para el acceso a Internet y para la desconexión, bloqueo, filtrado y otras restricciones de la red y sus contenidos». *Revista De Derecho Político*, 1(108), 2020, pp. 13-40. https://doi.org/10.5944/rdp.108.2020.27991

32 HLG-UE, *Informe final A multidimensional approach…cit.*

33 Comisión Europea, *Recomendación (UE) 2018/334, de 1 de marzo, sobre medidas para combatir eficazmente los contenidos ilícitos en línea,* 2018 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018H0334&from=FR

los desórdenes informativos en muchas ocasiones sí que son contenidos lícitos. También en la primera mitad de 2018, la Comisaria responsable amenazó a plataformas y agentes principales de que elaboraran un código de autorregulación, pues de lo contrario la UE regularía la materia.

Así, se adoptó el Código de buenas prácticas de octubre de 2018[34] que fue suscrito por las principales plataformas en línea, las principales redes sociales, los anunciantes y la industria de la publicidad. En el mismo, se comprometen a adoptar medidas de transparencia en la publicidad política, cierre de cuentas falsas, desmonetización de los proveedores de desinformación y en su anexo se identifican las mejores prácticas. Especialmente significativo es el sistema de exhaustivos informes periódicos que los firmantes han de presentar: en enero de 2019, informe de autoevaluación de octubre 2019, evaluación de septiembre de 2020 y un programa de control específico con el Covid en 2020[35]. Al momento de cerrar estas páginas se va a adoptar un Código de buenas prácticas reforzado en 2021 a partir nuevos compromisos de las partes y de las Orientaciones de la Comisión[36]. Se busca en esencia mejorar indicadores que permitan un mejor monitoreo y contar con mejores datos para investigadores; mejorar el contexto de la información con la visibilidad de la información fiable de interés público y de puntos de vista alternativos; dificultar la publicidad falsa o engañosa; establecer procedimientos y normas con verificadores así como limitar la amplificación artificial de las campañas de desinformación. El Grupo de Reguladores Europeos de los Servicios de Medios Audiovisuales también propone el modelo del código para este sector[37].

Asimismo, sería deseable integrar a más sujetos en estos mecanismos, en particular a las plataformas y empresas que facilitan la mensajería privada (*Whatssap, Telegram*, etc.) y tienen un especial papel frente a la viralización de contenidos. Bien es cierto que hay que adecuar las normas que se adopten al secreto de las comunicaciones y las expectativas razonables de privacidad de los usuarios.

La Recomendación 5949 del 12 de septiembre de 2018[38] asentó también las bases de la institucionalización y cooperación en la UE: propone la creación de redes nacionales en elecciones en las que también participen las autoridades

34 Unión Europea, *Código de buenas prácticas de la Unión en materia de desinformación*, UE, 2018, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59111

35 Comisión Europea, Información sobre *Code of Practice on Disinformation*, 2021, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

36 Comisión Europea, COM(2021) 262 final, *Orientaciones de la Comisión Europea sobre el refuerzo del Código de Buenas Prácticas en materia de Desinformación*, Bruselas, 26.5.2021, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021DC0262&from=EN

37 ERGA, *Report on Disinformation: Assessment of the implementation of the Code of Practice*, 4 de mayo 2020, https://erga-online.eu/?p=732

38 Comisión Europea, *Recomendación 5949 del 12 de septiembre de 2018*, Salzburgo, 19 y 20 de septiembre de 2018, https://ec.europa.eu/transparency/documents-register/detail?ref=C(2018)5949&lang=es

electorales; se impulsa un sistema de información rápido y de cooperación, en su caso europeo; debe designarse un punto de contacto único de los Estados y la Comisión. El enfoque de ciberseguridad es básico. Igualmente se insiste en la importancia de la transparencia de la propaganda electoral y la obligación de informar por partidos y organizaciones. De igual modo, se recuerda la proyección del régimen de protección de datos en la materia.

Esta actividad culminó en 2018 con el Plan de Acción contra la desinformación[39]. En esencia, se apuesta por el aumento de recursos, respuestas coordinadas tecnológicas y la implantación del *Rapid Alert System* (RAS), el Código de buenas prácticas y la creación de grupos para verificar y contrastar datos y concienciar.

Y desde finales de 2020 las acciones de la UE han cobrado nuevos e importantes impulsos. Así, la desinformación es un tema importante y transversal en el Plan de Acción para la Democracia Europea[40], publicado el 3 de diciembre de 2020. Además de un ecosistema digital más transparente y responsable, el fortalecimiento de medios, periodistas e investigadores, se busca fortalecer mecanismos como el RAS. El Plan también apuesta por impulsar más la aplicación del Reglamento general de protección de datos (RGPD) por la alfabetización mediática, la formación y la educación. Asimismo, el Plan apuesta por «más obligaciones y rendición de cuentas para las plataformas en línea» con compromisos claros y mecanismos de supervisión.

Al mismo tiempo que el Plan, el 15 de diciembre 2020, se presentó la propuesta de *Digital Services Act*, DSA, un ambicioso Reglamento de directa aplicación en toda la UE. Como luego se expone, se trata de un modelo de corregulación que incide sin duda en materia de desinformación. La DSA deja importantes espacios a la autorregulación, poder de control, moderación y políticas de uso de las plataformas, si bien a colmar también a través del Código de autorregulación reforzado. En todo caso y como se dirá, la futura DSA obliga a la implantación de mecanismos y normas internas y sistemas de resolución de conflictos e incluye obligaciones, supervisión y control.

Finalmente, tras un proceso de consulta pública[41] a fines de noviembre de 2021 la Comisión propondrá legislación para garantizar una mayor transparencia en el concreto ámbito de la publicidad política en plataformas, que más tarde se aborda.

Según se puede apreciar, la UE está dando una respuesta a este poliédrico fenómeno de la desinformación desde todos los ángulos que corresponden. Cualquier propuesta regulatoria en clave nacional ha de integrarse en el sistema de la

39 Consejo de la UE, *Plan de Acción contra la desinformación*, Bruselas, 12 de diciembre de 2018 https://data.consilium.europa.eu/doc/document/ST-15431-2018-INIT/es/pdf

40 Comisión Europea, C*omunicación COM(2020) 790 final, Plan de Acción para la Democracia Europea*, 3 de diciembre de 2020, en especial, apartado 4.º, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0790&from=ES

41 Comisión Europea, *Political advertising — improving transparency*, 2021, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12826-Political-advertising-improving-transparency_en

UE. Ello es especialmente importante para evitar la fragmentación y desarmonización. Regulaciones como la NetzDG de Alemania de 2017[42], las referidas leyes de Francia de 2018 y la ley francesa de 24 de junio 2020 para combatir el contenido que incita al odio en Internet (en buena medida declarada inconstitucional) o propuestas de ley como la de 15 de enero de 2021 de Polonia[43] sobre la protección de la libertad de expresión en las redes sociales en línea son negativas porque, como se ha afirmado desde el Parlamento de la UE, «esta tendencia crea un riesgo de fragmentación jurídica, mientras que las plataformas en línea prestan de facto servicios a escala de la UE.»[44]

Ahora bien, el sistema de la UE deja espacios no sólo a la autorregulación por las plataformas y redes, sino también a la regulación nacional que incluso debe potenciar y desarrollar el sistema. Así, se han de regular e implementar las estructuras internas gubernamentales que deben cooperar y compartir información. Asimismo, el marco de la UE y la futura DSA obligará a los Estados a regular y en su caso crear las diversas autoridades internas determinando sus atribuciones, su estatuto y fórmulas concretas de actuación. De igual modo, el ámbito de actuación nacional sigue siendo bastante amplio para articular las garantías ante las actuaciones frente a la desinformación. Así sucede con lo relativo al régimen electoral y sus instituciones y garantías, así como la determinación de las autoridades independientes a escala nacional y en lo relativo a la ponderación de los derechos fundamentales y libertades en juego, régimen de recursos, suspensiones de medidas y otras concretas garantías.

IV. LA REGULACIÓN DE LA DESINFORMACIÓN EN CLAVE INTERNACIONAL COMO OPERACIONES DE INFLUENCIA INDEBIDAS

Los fenómenos de desinformación pueden verse como operaciones indebidas de influencia («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») o de injerencia extranjera u operaciones híbridas» («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»).

42 *Gesetz Zur Verbesserung der Rechtsdurchsetzung in Sozialen Netzwerken* (Netzwerkdurchsetzungsgesetz-Netzdg). https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

43 https://www.gov.pl/attachment/5a0c5ba6-67cb-43af-ae38-aa5dc805e14f

44 Tambiama, M. — Parlamento UE, *Reform of the EU liability regime for online intermediaries. Background on the forthcoming digital services act*. In-depth analysis, EPRS (European Parliamentary Research Service), 2020, pp. 11-12, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2020)649404

Así se expresa en el mencionado Plan de Acción Europeo para la Democracia (n.º 4), siguiendo a Pamment[45] en el documento sueco, de referencia también para la OTAN[46]. Las campañas estructuradas de desinformación pueden ser una amenaza a la seguridad nacional e internacional[47]. Se trata de sistemas muy eficaces de política exterior para algunos países. Se desestabiliza y polariza internamente a las democracias occidentales y además las someten a contradicciones por cuanto las respuestas a la desinformación pueden ser contrarias a los propios principios democráticos y los derechos y libertades. Asimismo, los países que utilizan la desinformación por los general son más inmunes a ésta por cuanto controlan mucho más las plataformas, los medios y el flujo de información en sus países.

La Comisión de Venecia apuesta por que se adapte la normativa internacional específica al nuevo contexto tecnológico y desarrollando capacidades institucionales para combatir las ciberamenazas (principio 6.º), así como porque se fortalezca la cooperación internacional (principio 7), pero manteniendo un Internet abierto y neutral en elecciones (principio 3.º)[48].

No hay excesivos consensos en la materia desde el Derecho internacional[49]. Como punto de partida, en 2013, el Grupo de Expertos Gubernamentales (GGE) de las Naciones Unidas estableció el consenso de que el Derecho Internacional se aplica al ciberespacio, al igual que a otros ámbitos[50]. En 2015 se presentaron compromisos voluntarios no vinculantes de que los Estados no lleven a cabo ni apoyen a sabiendas actos ilícitos en el ciberespacio, incluidas acciones que dañen intencionadamente infraestructuras críticas o tengan como objetivo equipos de respuesta a emergencias informáticas[51]. De este modo, la injerencia electoral se aprecia como interferencia en una infraestructura, aunque las operaciones de información y la desinformación no se abordan directamente. En 2021 se hace una mera mención como problema emergente el «uso malintencionado por los Estados de campañas

45 Pamment, J., *The EU's Role in Fighting Disinformation: Taking Back the Initiative*, Washington DC: the Carnegie Endowment for International Peace, junio 2020, https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf

46 Pamment, J. et al., *The role of communicators in countering the malicious use of social media*, NATO STRATCOM COE, 2018, https://stratcomcoe.org/publications/the-role-of-communicators-in-countering-the-malicious-use-of-social-media/101

47 Cabe remitir a Gómez de Ágreda, Á., *Ética del ecosistema híbrido cognitivo entre el espacio físico y el ciberespacio. Aproximación desde el caso de la inteligencia artificial*, Tesis Doctoral, UPM, 2021. https://oa.upm.es/67495/

48 Comisión de Venecia, *Opinión 974/2019… cit*.

49 Al respecto, por todos, Robles Carrillo, M. «El régimen jurídico de las operaciones en el ciberespacio: estado del debate», *bie3: Boletín IEEE*, n.º 16, 2019, pp. 476-493, DOI: 10.17103/reei.39.07 y Faesen, L. *et al, Red Lines & Baselines… cit.* pp. 17 y ss. https://dialnet.unirioja.es/descarga/articulo/7461801.pdf

50 GGE-Naciones Unidas, *Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98*, 24.6. 2013.

51 GGE-Naciones Unidas-Rõigas, H. y Minárik, T., *UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*, CCDOE, 2015 https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/

de información encubiertas con ayuda de las TIC para influir en los procesos, los sistemas y la estabilidad general de otros Estados»[52]. Francia claramente ha señalado «cualquier penetración no autorizada de un Estado en los sistemas franceses o cualquier producción de efectos en el territorio francés a través de un vector digital puede constituir, como mínimo, una violación de la soberanía»[53].

Por cuanto a las facultades estatales de actuar frente a la desinformación desde el Derecho internacional, no parece haber dudas de que «un Estado ejerce control sobre la ciberinfraestructura y las actividades cibernéticas en su territorio, lo hace sobre la base del principio de soberanía.»[54]. Así pues, España como cualquier Estado soberano tiene la facultad de detectar, evaluar y combatir estas injerencias indebidas de otros Estados y debe abstenerse de realizarlas y, por tanto, de intervenir en asuntos internos de otros Estados. La actuación frente a estas campañas puede incluso considerarse el ejercicio a la legítima defensa a que refiere el artículo 51 de la Carta de Naciones Unidas. También en clave internacional, la Constitución de la Unión Internacional de Telecomunicaciones[55] en su artículo 34 expresa el derecho (de los Estados) a interrumpir, de acuerdo con su legislación nacional, otras telecomunicaciones privadas (esto es, no públicas) que puedan parecer peligrosas para la seguridad del Estado o contrarias a sus leyes, al orden público o a las buenas costumbres.» Basta la comunicación inmediata a los demás Estados de la UIT (art. 35 y art. 62 a). Ello, sin perjuicio de las obligaciones de Derecho internacional y que le prohíban hacerlo en un caso particular, como las normas de derechos humanos[56].

Ahora bien, en contra de la posición de las democracias occidentales, Rusia o China lideran un enfoque internacional seguido mayoritariamente de lo que se puede denominar «cibersoberanía». Se parte de que cualquier ataque a la soberanía puede ser abordado libremente incluyendo respuestas unilaterales de gobernanza de Internet (como *Rusnet* o la propia concepción china de Internet) y sin que deban tenerse en cuenta los derechos y libertades. Las regulaciones de estos países abordan el fenómeno bajo nociones de seguridad de la información, como sucede en el caso ruso.

Hay cierto espacio de consenso para afirmar en Derecho internacional una prohibición de campañas de desinformación extranjeras concertadas y las operaciones

52 GGE-Naciones Unidas, *Informe sobre el fomento de la conducta responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional*, Naciones Unidas, 14 de julio 2021, II. 9, p. 8 https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030S-1.pdf

53 Ministerio de Defensa de Francia, *International Law Applied to Operations in Cyberspace*, 2019, p. 7 (traducción libre) https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf#page=6

54 Schmitt, M. (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyberoperations*, (2.ª ed.) Cambridge University Press, 2017. Se sigue la regla 62 y comentarios en pp. 271 y ss.

55 UIT, *Constitución de la Unión Internacional de Telecomunicaciones*. Marrakech. 2002, https://www.itu.int/council/pd/constitution-s.docx

56 Schmitt, M. (dir.), *Tallinn Manual 2.0… cit.* art. 62. 1.º, y comentario 9.º.

de influencia encubiertas o la comunicación estratégica no transparente destinadas a socavar los procesos democráticos. Como se señala, la propaganda tipo RT de Rusia, o la BBC o CNN desde aquella perspectiva, sí que serían aceptables[57]. Así, se pone el acento en la conducta, medios e instrumentos y no tanto en los contenidos. Pues bien, las cosas han cambiado. Una vez cerrado este estudio, tras la invasión de Ucrania, la UE ha regulado la prohibición de emisiones desde Rusia[58]. Y sobre tal base la Comisión Europea ha ordenado a las plataformas el cierre de emisiones en Internet de canales como *Russia Today* y *Sputnik*. El Reglamento justifica la medida porque Rusia ha seguido una «sistemática» campaña de «manipulación y distorsión de los hechos» en su estrategia de desestabilización. Se afirma también una «propaganda» «repetida y constantemente dirigida a partidos políticos especialmente en periodos electorales» (Cons. 6 y 7). Se dice que los medios y canales mencionados están «bajo el control permanente o indirecto» de los líderes del gobierno ruso (Cons 8). Con la prohibición de emisiones se pretende el «cese de la propaganda» (Considerando 10). Pues bien, sin posibilidad de extenderme ahora, entiendo que la base jurídica y competencia para adoptar la medida es cuestionable, y más lo es su fondo: así deslegitima a la Unión Europea hacia el interior y el exterior y se abre una vía extremadamente peligrosa para el futuro.

En este punto cabe recordar que el CEDH reconoce «la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas [...] sin consideración de fronteras» (art. 10. 2 CEDH). A este respecto el Consejo de Europa en su Recomendación CM / Rec (2015) 6, ha recordado el «flujo libre y transfronterizo de información en internet»[59]. En consecuencia, «las medidas adoptadas por las autoridades estatales para combatir el contenido o las actividades ilegales en Internet no deben tener un impacto innecesario y desproporcionado más allá de las fronteras de ese Estado» (ap. 2.º). También su RecomendaciónCM / Rec (2011) 8 sobre la protección y promoción de la universalidad, integridad y apertura de Internet incluye la responsabilidad del Estado de garantizar que las acciones dentro de su jurisdicción no interfieran ilegítimamente con el acceso a la información en otros Estados o afecten negativamente el flujo transfronterizo de información en Internet[60].

En la UE se siguen líneas correctas de actuación: responsabilizar a concretas autoridades nacionales, que deben ser puntos únicos de contacto a nivel de la UE para compartir datos, información sobre detección y respuesta frente a campañas, conocimientos, herramientas y buenas prácticas. Asimismo se homogeneizan los

57 Faesen, L. *et al, Red Lines & Baselines… cit.* p. 22.

58 Medida articulada con el artículo 2 f) del Reglamento (UE) 833/2014 (modificado por Reglamento (UE) 2022/350 de 1 de marzo).

59 Consejo de Europa, *Recomendación CM / Rec (2015) 6 del Comité de Ministros a los Estados miembros Sobre el flujo libre y transfronterizo de información en Internet*, 1 de abril de 2015, https://search.coe.int/cm/Pages/result_details.aspx?Reference=CM/Rec(2015)6

60 Consejo de Europa, *Recomendación CM / Rec (2011) 8 sobre la protección y promoción de la universalidad, integridad y apertura de Internet*, 21 de septiembre 2011, n.º 1.1.1, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cc4d5

protocolos para este contacto y flujo de información. Así, desde marzo de 2019 está activo el *Rapid Alert System* (RAS), plataforma que conecta a los funcionarios («Puntos de contacto») que trabajan para abordar la desinformación de todos los Estados miembros de la UE y las instituciones y estructuras pertinentes de la UE. El sistema incluye un enlace a la Red Europea de Cooperación en materia de Elecciones (*European Cooperation Network on Elections*, ECNE) y la *Network Against Disinformation* de la Comisión. Cada Estado evalúa si una campaña de desinformación es relevante para generar una alerta a la UE. Además de las alertas, con el Covid se ha intensificado la actividad del RAS para diseñar un enfoque y una respuesta comunes.

Considero que en esta perspectiva internacional se ha de profundizar y seguir la estela de la UE y las políticas de cooperación deben extenderse para el ámbito ONU, OTAN, OCDE, etc. Hay que compartir información de manera rápida para poder dar respuestas rápidas. Se apuesta por estrategias de Puntos únicos de contacto o Centros de Análisis e Intercambio de Identificación de amenazas, Información Alerta y Asesoramiento público-privados. Los miembros de estos sistemas de cooperación rastrean, identifican, comparten información y establecen mecanismos de respuesta. También hay que establecer sistemas y lenguajes interoperables y comunes tanto para los humanos como para los sistemas automatizados[61]. Estos sistemas deben contar también con participación de la sociedad civil, expertos y académicos, así como mecanismos de transparencia que permitan el control. No olvidemos que errores o sesgos en la identificación y etiquetado de estas conductas y amenazas pueden llevar a cercenar masivamente contenidos perfectamente protegidos por la libertad de expresión e información.

V. MEDIDAS VOLUNTARIAMENTE ADOPTADAS POR LAS PLATAFORMAS, FENÓMENOS AUTORREGULATORIOS Y LA FUTURA DSA

1. **Medidas de las plataformas frente a la desinformación**

Las principales plataformas adoptan muchas medidas respecto de las campañas de desinformación[62]. Faesen y otros[63] sintetizan las normas principales que habrían de seguir las plataformas: transparencia de la política de las plataformas y de las definiciones que emplean; eliminación de cuentas de *bots* maliciosos, las redes de *bots* o el comportamiento inauténtico coordinado; medidas de verificación

61 Faesen, L. *et al, Red Lines & Baselines… cit.* pp. 66 y ss. y pp. 77 y ss.

62 CELE, Álvarez Ugarte, R. y Del Campo, A., *Noticias falsas en Internet: acciones y reacciones de tres plataformas*, Universidad de Palermo, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), febrero de 2021, https://www.palermo.edu/Archivos_content/2021/cele/papers/Desinformacion-y-acciones-de-plataformas-2021.pdf

63 Faesen, L. et al, *Red Lines & Baselines*… cit. pp. 36 y ss.)

de cuentas; procesos de comprobación de hechos contando con *fackt cheekers* acreditados; directrices estandarizadas para el sistema de etiquetado de contenidos de desinformación, de actores de la desinformación y de contenidos patrocinados. Respecto de algoritmos y moderación automática de contenidos, es necesaria la transparencia de su funcionamiento. Asimismo, hay que contar con mecanismo de denuncia y reclamación de usuarios y capacidad de apelación de sus decisiones.

Según un examen de la información disponible, *Facebook* cuenta con una política de comportamiento inauténtico coordinado[64] basado en identificar y actuar frente a pautas de comportamiento, vinculado a interferencias políticas y tácticas de participación. *Google*[65] hace referencia a operaciones de influencia y a las campañas de desinformación.

Las variadas políticas de *Facebook* se basan en eliminar, reducir e informar[66]. Se *elimina* el contenido que infringe sus políticas, se *reduce* la difusión del contenido problemático y se *informa* a las personas con información adicional y contexto. Se persigue el «fraude electoral o censal» y la «interferencia electoral o censal»[67]. También los anuncios que infrinjan las Políticas de Publicidad, incluidos los anuncios con afirmaciones desacreditadas por *fact-checkers*[68]. Se *reduce* el contenido problemático que definen sus Normas de distribución de contenido[69]. Por cuanto a la información y contextualización, *Facebook*[70] aplica etiquetas de desinformación de alerta de contenidos verificados como falsos, se advierte que se va a compartir un contenido etiquetado y en ocasiones remiten a información sobre Covid o electoral oficial. Por su parte, *Google*[71] realiza diversas actividades de contextualización, así como paneles informativos procedentes de *fact-checkers*. *Twitter*[72] también aplica contexto respecto de contenidos o reduce visibilidad a determinados contenidos, asimismo agrega etiquetas a contenidos multimedia

64 Facebook, *How We Respond to Inauthentic Behavior on Our Platforms: Policy Update*, 21 de octubre 2019, https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/

65 Google, *How Google Fights Disinformation,* 2019, https://kstatic.googleusercontent.com/files/388aa7d18189665e5f5579aef18e181c2d4283fb7b0d4691689dfd1bf92f7ac2ea6816e09c02eb98d-5501b8e5705ead65af653cdf94071c47361821e362da55b

66 Facebook, *Nuestro enfoque sobre la información errónea,* 29 de julio 2021 https://transparency.fb.com/es-es/features/approach-to-misinformation/

67 Facebook, *Organización de actos dañinos y fomento de actividades delictivas,* noviembre 2021, 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

68 Facebook, *12. Información errónea* (sin fecha), https://www.facebook.com/policies/ads/prohibited_content/misinformation

69 Facebook, *Normas de distribución de contenido. Tipos de contenido que penalizamos.* Septiembre 2021 https://transparency.fb.com/es-es/features/approach-to-ranking/types-of-content-we-demote/

70 Facebook, *Cómo funciona el programa de verificación de datos independiente de* Facebook. Junio 2021, https://www.facebook.com/journalismproject/programs/third-party-fact-checking/how-it-works

71 Google, *How Google Fights Disinformation*. 2019, https://kstatic.googleusercontent.com/files/388aa7d18189665e5f5579aef18e181c2d4283fb7b0d4691689dfd1bf92f7ac2ea6816e09c02eb98d-5501b8e5705ead65af653cdf94071c47361821e362da55b

72 Twitter, *Política relativa a los contenidos multimedia falsos y alterados*, (sin fecha), https://help.twitter.com/es/rules-and-policies/manipulated-media

falsos o alterados. Igualmente Twitter aplica etiquetas para dejar claro si se trata de cuenta oficial de Gobierno o de medios afiliados a un Estado[73].

Twitter desde enero de 2021 ha desarrollado una detallada «Política de integridad cívica»[74]. También actúa para evitar amplificar artificialmente información o manipular la plataforma[75]. No obstante, esta plataforma quizá tiene una visión más amplia y más centrada en contenidos que en conductas. La referida política prohíbe «manipular o interferir en elecciones u otros procesos cívicos. Esto incluye publicar o compartir contenido que pueda disuadir la participación o engañar a las personas sobre cuándo, dónde o cómo participar en un proceso cívico». Las medidas graduales pasan por etiquetar o reducir la visibilidad de los *tweets* que contengan información falsa o engañosa. Gradualmente se utilizan sistemas de advertencia, así como eliminaciones de *tweets*, modificaciones del perfil, etiquetas o bloqueos y suspensión permanente de la cuenta. Asimismo *Twitter*[76] cuenta con un archivo de operaciones de desinformación por entidades vinculadas con algunos Estados. Más adelante se hará referencia más concreta a las medidas relativas a la publicidad electoral.

2. **Modelos de autorregulación frente a regulaciones «fuertes» y la corregulación de la Digital Services Act**

Las actuaciones voluntarias de las plataformas y redes contra la desinformación, afortunadamente, son muy importantes. Ahora bien, no puede dejarse la cuestión totalmente a lo que ellas decidan ni en clave estratégica e internacional, ni respecto del ámbito electoral, ni en general. Sus intereses privados en modo alguno tienen por qué alinearse con los intereses nacionales[77] ni con los intereses públicos y derechos fundamentales de la ciudadanía en juego. De ahí que es necesario ver qué fórmulas de regulación emplear para hacer prevalecer tales intereses y derechos en juego.

Las legislaciones *fuertes* de los Estados o la UE serían las que establecen obligaciones y restricciones de contenidos o imponen concretas obligaciones de actuación a plataformas, intermediarios u otros actores implicados. Frente a ese modelo, los

73 Twitter, *Sobre las etiquetas en cuentas de medios afiliados al gobierno y al Estado en Twitter,* (sin fecha) https://help.twitter.com/es/rules-and-policies/state-affiliated

74 Twitter,. *Política de integridad cívica*, enero de 2021. https://help.twitter.com/es/rules-and-policies/election-integrity-policy

75 Twitter, *Política relativa al spam y la manipulación de la plataforma*, enero de 2021. https://help.twitter.com/es/rules-and-policies/platform-manipulation

76 Twitter, *Operaciones de información. Información sobre los intentos de manipulación de Twitter por parte de entidades que están vinculadas con ciertos Estados*, 2021, https://transparency.twitter.com/es_es/reports/information-operations.html

77 Carr, M., «Public-private partnerships in national cyber-security strategies», International Affairs 92, n.º 1 (enero de 2016), pp. 43-62. https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf y Faesen, L. *et al, Red Lines & Baselines… cit.* p. 12.

diversos modos de autorregulación tienen ventajas y cobran especial protagonismo en general en Internet y en particular en el ámbito de la desinformación. Entre estos modelos autorregulatorios estarían la corregulación, la llamada autorregulación regulada, los códigos de conducta, los sistemas de resolución de conflictos, las políticas y normas de uso de plataformas, las normas y estándares propios de los sectores implicados.

Son varias las ventajas que aportan estos sistemas autorregulatorios. Especialmente, atemperan los riesgos de impactar la libertad de expresión de usuarios, plataformas y redes así como de afectar la libertad empresarial de estas últimas. En este punto, se evitan mandatos sobre contenidos, si bien se delimita el poder de actuación y moderación de las plataformas. De igual modo, se pueden imponer obligaciones de transparencia y de garantías, con mecanismos de garantía y reclamación. Asimismo, la corregulación permite tomar como punto de partida las muchas actividades e inercias que ya adoptan las plataformas respecto de la desinformación y el fuerte avance que supone del Código de buenas prácticas de la UE, si bien, puede reconducir y estimular estas inercias. La corregulación también permite complementar las regulaciones que, como sucede con el actual texto de DSA, dejarán importantes aspectos por definir, además, muy sensibles para la libertad de expresión[78]. Estos modelos autorregulatorios también aseguran la mayor eficacia de lo regulado y su implantación efectiva. De igual manera, estos modelos evitan otros modelos como el de cibersoberanía ruso.

La futura DSA establece claramente un modelo de corregulación[79]. Viene a suponer una norma «fuerte» que respalda y mantiene el poder y las propias normas y acciones de las plataformas. Se regulan los principios básicos, que han de concretar y hacer efectivos las propias plataformas, que además son las que han de articular los medios. En este sistema se estimula la adopción de códigos de conducta (Cons. 68-69, art. 35 DSA) y se regulan los instrumentos, herramientas y órganos de garantía.

En la DSA hay previsiones en materia de «evaluación de riesgos sistémicos» de muy grandes plataformas (arts. 25 y ss.), vía por la que se van a introducir nuevas obligaciones, algunas de ellas vinculadas precisamente a la evitación de determinadas formas de desinformación. A partir de estas evaluaciones las plataformas habrán de adoptar medidas de reducción de riesgos (art. 27) o realizar auditorías independientes (art. 28), que no están aún definidas y, ciertamente, pueden ser polémicas desde la libertad de expresión. La DSA también contiene previsiones que imponen garantías del debido proceso, tutela y reclamación frente a las decisiones de las plataformas, que bien pueden estar vinculadas al ámbito de la

78 Barata, J., *The Digital Services Act and its impact on the right to freedom of expression: special focus on risk mitigation obligations*, PLI, Plataforma por la Libertad de Información, junio 2021. https://libertadinformacion.cc/wp-content/uploads/2021/06/DSA-AND-ITS-IMPACT-ON-FREEDOM-OF-EXPRESSION-JOAN-BARATA-PDLI.pdf

79 Faesen, L. *et al., Red Lines & Baselines… cit.* p. 57.

desinformación. Por cuanto a la transparencia, las plataformas habrían de dar información sobre las órdenes gubernamentales que reciban para que actúen contra contenidos ilícitos (art. 8) relacionados con la desinformación y brindar informes de transparencia (art. 9) sobre decisiones adoptadas.

En la futura DSA hay que destacar el importante papel regulador de las autoridades nacionales («coordinadores de servicios digitales» de los Estados, arts. 38 y ss.) y la futura Junta Europea de Servicios Digitales. Como se ha adelantado, su papel será esencial con amplias competencias de regulador para determinar criterios y estándares, dictar órdenes de actuación, poderes de monitoreo e inspección, sanciones, medidas provisionales, etc. Asimismo serán autoridad independiente estatal a la que puedan acudir los usuarios con reclamaciones frente a las plataformas (art. 43). Los coordinadores también certificarán en los Estados a los órganos de resolución de conflictos (art. 18), así como a los alertadores fiables de contenidos ilícitos (art. 19). Todo ello puede tener clara proyección en el ámbito de la desinformación. La futura importancia de estos coordinadores de servicios digitales obliga a estar muy vigilantes de que se cumplan los mandatos de independencia (art. 39).

VI. PROTECCIÓN Y DEFENSA DEL PERIODISMO Y LA (AUTO) REGULACIÓN DE LA VERIFICACIÓN DE NOTICIAS

Frente a la desinformación es esencial la potenciación de la transparencia del ecosistema de la información, incluyendo a los medios periodísticos, salvaguardar la diversidad y la sostenibilidad del ecosistema europeo de medios de comunicación. Así se ha insistido en los ya referidos Informe final del Grupo de expertos y el Plan de Acción para la Democracia Europea. 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[80]. No obstante, desde el enfoque jurídico normativo que aquí se sigue es difícil hacer propuestas regulatorias concretas al respecto. Debe también tenerse en cuenta al respecto la Resolución sobre la ética del periodismo del Consejo de Europa (1993), conocida como Código Europeo de Deontología del Periodismo[81]. 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

80 Comisión Europea, *Recommendation on the protection, safety and empowerment of journalists*, 16 September 2021. https://digital-strategy.ec.europa.eu/en/library/recommendation-protection-safety-and-empowerment-journalists

81 Consejo de Europea, *Resolución Asamblea parlamentaria. Código Europeo de Deontología del Periodismo*. Estrasburgo: 1 de julio de 1993, http://periodistasandalucia.es/wp-content/uploads/2017/01/CodigoEuropeo.pdf

la garantía para su cumplimiento de la Comisión de Arbitraje Quejas y Deontología del Periodismo.

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[82]. Su actividad está protegida por la propia libertad de expresión e información y forma parte de la deliberación que es propia a una sociedad democrática. No obstante, estas organizaciones necesitan contar con una especial legitimación social para su efectividad. Por ello, los *fact-checkers* han de cumplir con especiales requisitos para distinguirse de otros medios o sujetos y para que la ciudadanía sepa cómo funcionan y actúan y si tienen una especial neutralidad.

Pues bien, es especialmente valiosa la experiencia de autorregulación del Código de Principios de la *International Fact-checking Network* (IFCN)[83], 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*. Se exige un compromiso con el apartidismo y la equidad, la transparencia de las fuentes y de las cuentas, la transparencia de financiación y organización y la transparencia de la metodología, con un particular compromiso con las correcciones abiertas y honestas. Como punto de partida y como es obvio, no se verifican opiniones, sino informaciones basadas en hechos. Resulta de especial interés conocer los acuerdos que tienen con las plataformas digitales para que puedan usar sus contenidos para identificar desinformación o dar mejor contexto. Ya se han desarrollado unos criterios muy concretos de aplicación de esté Código de principios[84]. Las entidades que se adhieren a este código anualmente deben ser evaluadas por un asesor independiente siguiendo estos criterios y tal evaluación es votada por un Consejo Asesor a nivel mundial[85].

En España fue rechazada una Proposición de Ley Orgánica, de 26 de junio de 2020 sobre verificación por el Grupo parlamentario de VOX[86]. En la misma se pretendía asegurar que la verificación de noticias falsas «sólo puedan llevarla a cabo personas y entidades no partidistas y/o partidarias ni dependientes, salvo que el titular de la red social, blog, sitio web en general, prensa impresa y digital, o medio audiovisual (radio y televisión), declare públicamente el carácter partidista

82 Al respect, Hameleers, M. y Van der Meer, Toni. G., «Misinformation and polarization in a high-choice media environment: How effective are political fact-checkers?». *Communication Research*, *47*(2), 2020, pp. 227-250, https://journals.sagepub.com/doi/pdf/10.1177/0093650218819671

83 IFCN, *Code of principles*, 2016, https://www.ifcncodeofprinciples.poynter.org/

84 IFCN, *Guidelines for applications: the IFCN code of principles*, (sin fecha), https://drive.google.com/file/d/1e-A_AmU3B3G8cbC9NfKSY0nH1zfWeH67/view

85 IFCN (s.f.). *Application process for the IFCN code of principles*, (sin fecha), https://www.ifcncodeofprinciples.poynter.org/process

86 Grupo VOX, *Congreso de los Diputados. Proposición 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*, 2020, https://www.congreso.es/busqueda-de-publicaciones?p_p_id=publicaciones&p_p_lifecycle=0&p_p_state=-normal&p_p_mode=view&_publicaciones_mode=mostrarTextoIntegro&_publicaciones_legislatura=XIV&_publicaciones_id_texto=(BOCG-14-B-95-1.CODI.)

y/o partidario y/o dependiente de tales medios digitales, impresos o audiovisuales». También se afirmaba «la prohibición de la verificación de noticias falsas por las autoridades gubernativas» y «de toda verificación de opiniones». Se disponía asimismo la posible responsabilidad civil por la acción de verificación y la legitimación para impugnar por todo usuario o lector. Quizá lo más discutible de la propuesta pasa por cuanto «Solo la autoridad judicial competente podrá adoptar decisiones sobre la verificación de noticias» (art. 3).

Considero que las líneas apuntadas en esta proposición pueden ser acogidas, si bien es cuestionable la necesidad de una regulación *fuerte* de esta cuestión a través de leyes. La materia puede encajar mejor a través de normas internas o códigos de medios de comunicación o redes. Estos instrumentos pueden ser eficaces para lograr los objetivos básicos en los medios y plataformas que ejerzan actividades de verificación. Y los objetivos a perseguir son: la obligatoriedad de identificación específica de toda acción que se autodenomine de verificación. Que si se da esta autodenominación, debe imponerse la obligación de informar si se forma parte o no de algún sistema autorregulatorio o código de conducta (como el IFCN) que imponga el cumplimiento de estándares y garantías de la acción de verificación. A través de la autorregulación habrían de imponerse también obligaciones específicas de transparencia respecto de la metodología seguida en la selección de noticias a verificar. Y en todo caso, por la vía de la autorregulación y en este caso sí pueden tener mayor cabidas regulaciones legales para establecer restricciones u obligaciones específicas a organismos y medios públicos que hacen la función de verificación. Incluso se puede regular la especial prohibición de su actividad calificada como de verificación de noticias en periodo electoral.

VII. ALGUNAS INERCIAS REGULATORIAS EN ESPAÑA

Acertadamente, desde la Estrategia de Seguridad Nacional 2017[87] se incluyen los ciberataques y las campañas de desinformación. El 19 de diciembre de 2017 hubo una proposición no de ley del Grupo Popular[88] por la que el Congreso instaba al Gobierno a adoptar «medidas de acción que garanticen la detección de esas informaciones en base a un buen método para identificarlas y su «sellado» o descalificación como potencial noticia falsa ante el ciudadano», además de introducir capacidades en los servicios de seguridad. La referencia al «sellado» no fue

87 Presidencia de Gobierno, *Estrategia de Seguridad Nacional*, 2017 https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf

88 Grupo Popular, *Congreso de los Diputados. Proposición no de Ley relativa al impulso de las medidas necesarias para garantizar la veracidad de las informaciones que circulan por servicios conectados a Internet y evitar injerencias que pongan en peligro la estabilidad institucional en España*, 19 de diciembre 2017, https://www.congreso.es/web/guest/busqueda-de-iniciativas?p_p_id=iniciativas&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_iniciativas_mode=mostrarDetalle&_iniciativas_legislatura=XII&_iniciativas_id=162%2F000550

bien aceptada y el Grupo Socialista propuso una enmienda[89] eliminando tal referencia que fue aceptada también por el Grupo de Ciudadanos.

También en 2017 se dio una Proposición no de ley socialista de derechos digitales y veracidad de las informaciones de 27 de marzo de 2017[90]. Esta proposición fue retomada en la tramitación de la LO 3/2018 de protección de datos a través de una enmienda de dicho grupo. Se pretendía que la ley afirmara 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[91] y el precepto finalmente adoptado limitó mucho su campo de acción al ser sólo relativo al derecho de rectificación en Internet (artículo 85). Este precepto instaba a adoptar necesarios «protocolos adecuados para posibilitar» el ejercicio de este derecho. Y pasados más de tres años, no se detecta ninguna actividad para que se haya hecho posible este derecho. Y nadie parece haberlo echado en falta.

Sin tratarse de un texto de carácter normativo, cabe mencionar la Carta de Derechos digitales adoptada en julio de 2021[92]. Su artículo XV sobre el derecho a recibir libremente información veraz habla de «promover la adopción» de estos protocolos a los que hace referencia la Ley orgánica 3/2018. Asimismo, la Carta subraya las garantías de la transparencia e información a los usuarios sobre si estos protocolos utilizan sistemas automatizados, técnicas de perfilado y el patrocinio de la información (XV 1 y 2). También, se reitera el derecho de rectificación o el aviso de actualización (XV. 3 a y b).

En 2018 en el contexto de la *liberación* de información en el *caso Villarejo*, la entonces Vicepresidenta del Gobierno Carmen Calvo en la XVI Jornada de Periodismo de la Asociación de Periodistas Europeos afirmó que se iba a regular el fenómeno de la desinformación en una línea restrictiva de la libertad de información, «para proteger los bienes superiores y colectivos frente a los bienes individuales»[93]. Afortunadamente, no se hizo nada. Según se acaba de señalar *infra*, en 2020 se rechazó una proposición de ley sobre verificadores por el Grupo VOX.

89 Grupo Socialista, Congreso de los Diputados. Enmienda. *BOCG*, 21.3.2018. https://www.congreso.es/web/guest/busqueda-de-publicaciones?p_p_id=publicaciones&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_publicaciones_mode=mostrarTextoIntegro&_publicaciones_legislatura=XII&_publicaciones_id_texto=(BOCG-12-D-322.CODI.)

90 Grupo Socialista, *Congreso de los Diputados. Proposición no de ley de derechos digitales y veracidad de las informaciones*, 27 de marzo de 2017, https://www.congreso.es/public_oficiales/L12/CONG/BOCG/D/BOCG-12-D-139.PDF

91 PLI, «La Pdli alerta sobre la propuesta del PSOE de regular los contenidos de internet: «no queremos un ministerio de la verdad», *PLI*, julio 2018 http://libertadinformacion.cc/la-pdli-alerta-sobre-la-propuesta-del-psoe-de-regular-los-contenidos-de-internet-no-queremos-un-ministerio-de-la-verdad/

92 Gobierno de España-De la Quadra, T. (coord.), *Carta de Derechos digitales*, julio de 2021. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

93 Piña, R., «El Gobierno apuesta por regular la libertad de expresión de los medios», *El Mundo,* 27 de septiembre 2018, https://www.elmundo.es/television/2018/09/27/5bacaf75468aebb25f8b463b.html

VIII. LA DESINFORMACIÓN BAJO LA OPACA REGULACIÓN ESPAÑOLA DE LA SEGURIDAD DE LA INFORMACIÓN Y EL «DECRETAZO DIGITAL»

Desde el punto de vista interno español, hay que tener en cuenta el contexto normativo de la ciberseguridad y ciberdefensa que puede estar vinculado o ser aplicable al fenómeno de la desinformación. Así, en especial cabe mencionar, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (y las «TIC» lo son, art. 2 y Anexo I). Especialmente destaca la Directiva 2016/1148, de 6 de julio, Directiva NIS (*Security of Network and Information Systems*) de la UE y su transposición en España (Real Decreto-ley 12/2018 y, recientemente, Real Decreto 43/2021). Se trata de una normativa compleja (Robles, 2021)[94]. Como he señalado en otro lugar[95], es un conjunto normativo en la *sombra* de la regulación de seguridad y bajo la *opacidad* de la regulación técnica. Deliberadamente no se suele regular con claridad el alcance de las restricciones y obligaciones que puede implicar. Ya se ha señalado que no es extraño en el mundo que la regulación de la desinformación quede en este contexto de la regulación de seguridad de la información. Es por ello que pese a la enorme trascendencia que pueden tener las medidas que se adopten bajo esta normativa, en buena medida pasa desapercibida incluso para los especialistas.

La referida normativa europea y española en principio no está pensada para aplicarse a amenazas y riesgos de desinformación a través de grandes redes y plataformas. Pero no hay que excluirlo. En principio, aunque puede ser discutible, hay que partir de que un intermediario, plataforma o red social puede ser considerados «operador de servicios esenciales». En consecuencia, pueden entenderse sujetos a las obligaciones de adoptar medidas de seguridad, detección de incidentes, contar con responsables de seguridad, sistemas de respuesta, así como, especialmente, estar obligados a notificar a las autoridades incidentes perturbadores significativos en sus servicios.

Sería de interés que la normativa española detallara su aplicabilidad para el concreto ámbito de plataformas y redes sociales y, en particular, la trascendencia que podría tener su aplicación incluso para afectar acceso a la información por la ciudadanía, así como las obligaciones de control y restricciones de información que puede implicar a los intermediarios.

94 Robles Castillo, M. «Análisis de la Normativa sobre Seguridad de Redes y Sistemas de Información: el Real Decreto 43/2021» en Serrano, M. A. et al. *Investigación en ciberseguridad. Actas de las VI Jornadas Nacionales de Ciberseguridad (JNIC2021 LIVE),* Universidad Castilla-La Mancha, 9-10 de junio de 2021, https://orcid.org/0000-0002-6324-4665

95 Cotino Hueso, L., «La (in)constitucionalidad de la «intervención», «mordaza» o «apagón» de las telecomunicaciones e internet por el Gobierno en virtud del Real Decreto-Ley 14/2019», en *Revista General de Derecho Administrativo*, *RGDA Iustel*, n.º 54 mayo 2020.

Atención especial merece el Real Decreto-Ley 14/2019, conocido como «decretazo digital», especialmente por cuanto modificó el artículo 4. 6.º Ley 9/2014, Ley General de Telecomunicaciones. En otro lugar he afirmado la inconstitucionalidad de esta regulación, como también lo ha hecho el Consell de Garanties Estatutaries[96]. El Tribunal Constitucional ha admitido un recurso de inconstitucionalidad del Gobierno Vasco[97] frente al mismo y hay que esperar una reforma de esta normativa tan peligrosa para la libertad de expresión. Y es que esta norma permite la intervención y control gubernamental de «redes y servicios de comunicaciones electrónicas» en aras de la seguridad pública y nacional. Con un lenguaje críptico, permite intervenir cualquier «cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario» (art. 4.6.º). Pues bien, esta regulación puede quedar vinculada al fenómeno de la desinformación. De hecho, su origen fue una reacción al uso político de redes en el contexto independentista en Cataluña que puso en peligro infraestructuras y la seguridad en España. Considero que es precisa una reforma de esta ley que: concrete mejor los presupuestos de aplicación, el alcance de las acciones que puede imponer el Gobierno y a quiénes, que especifique los mecanismos y los órganos de garantías, con controles por autoridades judiciales ya previos, inmediatos o, en su caso, a posteriori. Sin embargo, la regulación actual, además de haberse adoptado a través de Decreto-Ley, no cumple los mínimos estándares de calidad normativa ni cuenta con las mínimas garantías de la libertad de expresión e información en Internet establecidas por el CEDH y las que cabe deducir de la Constitución española.

IX. REGULACIÓN INSTITUCIONAL Y ORGÁNICA DE LA DESINFORMACIÓN Y LA ORDEN DE 2020

En España hay que destacar la Orden PCM/1030/2020, de 30 de octubre, sobre el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. Esta Orden determina los objetivos (punto 2): identificar las instituciones y órganos con atribuciones, establecer unos niveles de actuación y cometidos en cada nivel; definir mecanismos para el intercambio de información sobre campañas de desinformación, buenas prácticas y procedimientos en la detección, para la evaluación del funcionamiento del procedimiento, una metodología para identificar y gestionar eventos, proponer equipos de trabajo para una futura «Estrategia Nacional de Lucha contra la Desinformación». En el marco del Sistema de Seguridad Nacional, se da una composición específica para

96 *Ibídem*. Consell de Garanties Estatutaries de Cataluña, *Dictamen 6/2019, de 30 de diciembre*, 2020, https://dogc.gencat.cat/es/document-del-dogc/index.html?documentId=889581

97 https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2021_044/NOTAINFORMATIVAN%C2%BA44-2021.pdf

la lucha contra la desinformación que cuenta con el Consejo de Seguridad Nacional, Comité de Situación, Secretaría de Estado de Comunicación, Comisión Permanente contra la desinformación y también se hace referencia a diversas «Autoridades públicas competentes», como el CNI y el «sector privado y la sociedad civil». Según el nivel de activación se implican los niveles técnicos o de gestión política y en su caso la activación de células de Coordinación e incluso del Consejo de Seguridad Nacional.

Tras el aluvión de críticas políticas y recursos que recibió el Gobierno por la Orden, el Vice-Presidente Comisión Europea Jourová le dio un respaldo señalando que iba en la línea de fortalecer las capacidades estatales en la lucha contra la desinformación[98]. La reciente sentencia del Tribunal Supremo de 18 de octubre de 2021 ha inadmitido el recurso presentado frente a la Orden[99]. El TS aprecia positivamente los objetivos de la orden y se sostiene que el Consejo de Seguridad Nacional está normativamente apoderado para elaborar y aprobar un instrumento de actuación con facultades de coordinación. Por lo que más interesa, acierta el TS cuando subraya que «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».

Como se ha adelantado en clave internacional, resulta preciso 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 bajo el enfoque de la ciberseguridad y la ciberdefensa. En esta misma línea, también debe existir una mayor coordinación de acciones de respuesta técnica y política 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. Asimismo, la regulación orgánica, competencial y funcional de las instituciones internas españolas también es necesaria para articular la acción concertada con la UE, especialmente por cuanto al sistema de alerta rápida y constituirse en puntos únicos de contacto y, en su caso, en otros marcos internacionales.

Es por ello que la referida Orden es un primer paso positivo en esta línea que, como el TS insiste, no regula contenidos ni atisba ningún tipo de restricción. Ahora bien, dada la especial sensibilidad social y política en la materia es muy importante que las actividades gubernamentales en la lucha contra la desinformación cuenten con una regulación y mecanismos de gobernanza, rendición de

98 Vice-Presidente Comisión Europea-Jourová, Contestación a pregunta E-006087/2020, Parlamento de la UE, 15 de febrero 2021, https://www.europarl.europa.eu/doceo/document/E-9-2020-006087-ASW_EN.html; Pregunta de 10 de noviembre de 2020 de Maite Pagazaurtundúa: https://www.europarl.europa.eu/doceo/document/E-9-2020-006087_EN.html

99 STS n.º 1240/2021, 18 de octubre de 2021 Sala de lo Contencioso, Sección 4, Rec 361/2020. https://delajusticia.com/wp-content/uploads/2021/11/STSinform.pdf

cuentas, transparencia y control reforzados. Así, para una mejor institucionalización se debería regular la periodicidad de actuación de estos órganos, así como su transparencia, por ejemplo, obligando a la realización de informes específicos y determinando la publicidad de los mismos. También cabría aclararse si la información o documentación generada tiene en su caso una particular reserva y confidencialidad. Debería esclarecerse la aplicación de la Ley 19/2013 bajo el principio de máxima transparencia. Así, la regulación o prácticas de estos órganos contra la desinformación deben incorporar una visión restrictiva de las causas de inadmisión de solicitudes de información (art. 18) así como de los límites aplicables a las solicitudes en razón del artículo 14, que potencialmente es claramente aplicable (defensa, seguridad, relaciones exteriores, prevención delitos, vigilancia, inspección y control, intereses económicos, confidencialidad…). Hay motivos específicos para que toda la información que se genera y fluya en estos órganos no sea accesible por todos. En malas manos podría servir para que quienes generan desinformación puedan eludir o limitar la eficacia de los protocolos y sistemas de identificación y respuesta. No obstante, este riesgo no puede llevar a una opacidad generalizada. Sin conocimiento de lo que hace el Estado contra la desinformación, cualquier garantía de los derechos se hace imposible por ser inatacable.

Desde el punto de vista de la gobernanza, hay que estimular la participación de la sociedad civil, sectores afines a la materia, la academia y expertos, no sólo por la calidad de sus contribuciones sino también como garantía de transparencia de las acciones que se adopten. 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.

X. PROPUESTAS REGULATORIAS PARA EL ÁMBITO ELECTORAL

1. **Necesidad de regulación española para el ámbito electoral**

El fenómeno de la desinformación, como explican Balaguer o Barrilao, tensiona al sistema constitucional y afecta a la democracia[100]. Y más específicamente a los procesos electorales, en los que las amenazas a la integridad de las elecciones se hacen más intensas[101]. Pero en estos contextos también es mayor el riesgo de que las medidas y regulaciones que se adopten impacten más en los derechos y

100 Balaguer Callejón, F., «Redes sociales, compañías tecnológicas y democracia», *Revista de derecho constitucional europeo*, n.º 32, 2019, https://www.ugr.es/~redce/REDCE32/articulos/04_F_BALAGUER.htm; Sánchez Barrilao. J. F. «Sociedad del miedo y desafección constitucional», Revista de derecho político, n.º 108, 2020, pp. 97-126 y «El Internet en la era Trump: aproximación constitucional a una nueva realidad», *Estudios en derecho a la información*, n.º 9, 2020, pp. 49-84.

101 Rubio Núñez, R., «Los efectos de la posverdad en la democracia». *Revista De Derecho Político*, 1(103), 2018, pp. 191-228. https://doi.org/10.5944/rdp.103.2018.23201

libertades. Tales medidas han de tener en cuenta y respetar el esencial papel de Internet, plataformas y redes para la conformación de la opinión pública. No se puede obviar la relevancia y el interés público de la publicidad y propaganda política, especialmente protegidos por la libertad de expresión por su importancia para los procesos democráticos y electorales.

La Comisión de Venecia señala que se ha de revisar la normativa «sobre la responsabilidad de los intermediarios para preservar la integridad electoral» (principio 5.º), si bien también predica la colaboración público privada y los mecanismos de autorregulación (principios 7.º y 8.º)[102]. Resulta preciso reforzar, estructurar y normalizar la transparencia de las plataformas en sus actuaciones. Y también la regulación debe aclarar las garantías específicas y en su caso recurribilidad, bien frente a las propias plataformas o los sistemas de resolución de controversias, bien los recursos ante las autoridades competentes.

Las garantías de transparencia y debido proceso son importantes en cualquier periodo, pero cuentan con una protección constitucional más intensa en periodo electoral. La legislación española debería regularlas expresamente. En esta dirección, cabe dotar a la Junta Electoral y, en su caso, a los tribunales competentes en el ámbito electoral de capacidad de respuesta ante la desinformación, así como dotarles de recursos materiales y técnicos suficientes. La legislación debe expresar atribuciones claras para adoptar decisiones eficaces y ágiles como requiere el periodo electoral, también en colaboración con las plataformas. Así, la regulación electoral (art 19 Ley Orgánica 5/1985) podría dejar aún más claras las capacidades de actuación y competencias de la Junta Electoral a resultas de consultas, requerimientos y reclamaciones de partidos y candidatos electorales. Por lo que interesa, respecto de las plataformas y redes cabe expresar las facultades de requerirles en periodo electoral con relación a las medidas que hayan adoptado. Cabe recordar a este respecto la reclamación de Unidas Podemos frente a *Facebook, Google* y *Whatsapp* por las restricciones del servicio en las elecciones generales de 28 de abril de 2019, que en aquel caso fueron rechazadas por la Junta Electoral Central (2019)[103]. En 2021 la Junta Electoral[104] ha tenido que hacer piruetas para declararse competente. No puede desconocer «la posición predominante de Twitter en la sociedad actual ha llevado a que en las campañas electorales constituya un instrumento casi imprescindible para candidatos y formaciones electorales». La Junta se afirma como competente para evaluar la razonabilidad de la medida respecto del derecho

102 Comisión de Venecia, *Opinión 974/2019… cit.*

103 Junta Electoral Central, *Acuerdo 300/2019, de 9 de mayo de 2019. Podemos v. Facebook, Google y Whatsapp, Expediente: 293/1006*, http://www.juntaelectoralcentral.es/cs/jec/doctrina/acuerdos?anyosesion=2019&idacuerdoinstruccion=68015&idsesion=936&template=Doctrina/JEC_Detalle

104 Junta Electoral Central, *Acuerdo 146/2021, de 25 de febrero de 2021, Expediente: 293/1215, Reclamación contra Twitter por la suspensión de la cuenta de VOX*. http://www.juntaelectoralcentral.es/cs/jec/doctrina/acuerdos?anyosesion=2021&idacuerdoinstruccion=75595&idsesion=992&template=Doctrina/JEC_Detalle

de participación política en condiciones de igualdad. Además, la Junta aprovecha (FJ 9.º) para pedir al legislador que regule por los «peligros y riesgos que pueden suponer algunas decisiones de los responsables de las redes sociales durante la campaña electoral» que «pueden limitar seriamente la campaña electoral de cualquier candidato», sin «apenas tendrá tiempo para obtener una tutela judicial eficaz». La Junta se manifiesta en contra de que «se adopten de plano sin oír con carácter previo a las personas perjudicadas». La STS de 28 de febrero de 2022 ha desestimado el recurso de VOX frente a la JEC, recordando, en cualquier caso que «insatisfactoria es, también por su escasez, la regulación de la potestad de control atribuida a la Administración electoral».

La normativa habría de expresar asimismo las obligaciones de respuesta y plazos a las que deben someterse las plataformas e incluso las consecuencias posibles de no hacerlo. La Comisión de Venecia (principio 2.º) afirma que «los órganos electorales puedan exigir a las empresas privadas que eliminen contenido de internet según las leyes». En sentido inverso, las autoridades independientes pueden obligar a revertir las medidas que hayan adoptado las redes y plataformas y atribuir garantías especiales para partidos y candidatos electorales frente a sus actuaciones.

Por otra parte, las actuales limitaciones temporales de la jornada de reflexión (artículo 53 Ley Orgánica 5/1985) y, especialmente la prohibición de publicar encuestas cinco días antes (artículo 69.7 Ley Orgánica 5/1985) deben replantearse. Estas prohibiciones pueden fomentar la aparición de desinformación. Además, su masivo incumplimiento deslegitima el propio sistema electoral.

Aunque al lector le pueda sorprender, desde hace muchos años en España se vive la ficción de que los partidos y candidatos electorales no pueden utilizar «ningún tipo de contratación comercial para su realización», con referencia al uso de redes sociales o Internet fuera del periodo de campaña electoral[105]. La formal inexistencia de relación jurídica entre partidos y redes fuera de periodo electoral dificulta totalmente su normalización y control jurídico y es preciso regular la materia.

2. **Algunas regulaciones comparadas de las que aprender y de las que no**

En el ámbito comparado un modelo positivo a tener en cuenta en el contexto electoral español es el «Protocolo público de incidentes electorales críticos»[106] en

105 Junta Electoral Central, *Instrucción 3/2011, de 24 de marzo, sobre interpretación de la prohibición de realización de campaña electoral incluida en el artículo* 53, http://www.juntaelectoralcentral.es/cs/jec/doctrina/buscadorresult?acuerdotexto=facebook&esinstruccion=false&idacuerdoinstruccion=25785&materias=0&operadoracuerdo=-1&operadorobjeto=-1&procesosElectorales=0&sPag=2&template=Doctrina/JEC_Detalle&tiposautor=0&total=19

106 Gobierno de Canadá, *Cabinet Directive on the Critical Election Incident Public Protocol*, marzo de 2019, actualizado en 2021. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol/cabinet.html

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 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. Pero, además, 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.

Por el contrario, frente a influencias indebidas otros modelos regulatorios que conllevan la restricción de emisiones o bloqueo de contenidos son especialmente cuestionables. De un lado, pueden ser de dudosa utilidad. Así sucede en Canadá (la *Elections Modernization Act*, de 13 de diciembre de 2018 (BILL C-76) regula la *Undue influence by foreigners* 282. 4 (1)[107]. 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.

En cualquier caso, en el panorama comparado destaca la ya referida Ley n.º 2018-1202 de 22 de diciembre de 2018 francesa. La misma no es un modelo suficientemente probado ni trasladable a España y, cuanto menos, habría que analizar más detenidamente sus cuestionables efectos. No es fácil valorar la aplicación de una ley que ha llevado a que *Twitter* bloqueara como desinformación un anuncio del Gobierno Francés[108] o que *Google* prohibiera en Francia durante la campaña publicar cualquier anuncio sobre debates de interés general[109]. Entre otras cosas, esta ley introduce un artículo 33-1-1 en la Ley n.º 86-1067 del 30 de septiembre de 1986 por el que el *Conseil supérieur de l'audiovisuel* en tres meses antes de elecciones tiene facultades para suspender emisiones de contenidos que

107 «https://digital-strategy.ec.europa.eu/en/library/recommendation-protection-safety-and-empowerment-journalists» https://digital-strategy.ec.europa.e

108 Euronews, «Twitter blocks French government ad campaign using France's own fake news law», 3 de abril de 2019. https://www.euronews.com/2019/04/03/twitter-blocks-french-government-ad-campaign-using-france-s-own-fake-news-law

109 Google, *Actualización de la política sobre contenido de carácter político (junio del 2020).* Abril. https://support.google.com/adspolicy/answer/9832056?hl=es

son consecuencia de acuerdos con Estados extranjeros o están realizados «bajo su influencia». El *Conseil supérieur* también puede avisar y obligar a que los 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.» Como punto de partida, puede ser de interés reconocer a las autoridades atribuciones excepcionales en periodo electoral. Pero la ley debería establecer claramente los presupuestos, las medidas concretas a adoptar y, especialmente, debería dejar en manos estas facultades expresamente a órganos de naturaleza judicial o claramente independientes, como puede ser en España la Junta y siempre con suficientes cautelas y transparencia.

Asimismo, el artículo L. 163-2.-I. dispone que cualquier partido, candidato o persona puede acudir a un juez especial único en Francia para solicitar que se retire una información difundida automatizadamente que sea inexacta o engañosa y que pueda afectar a las elecciones a través de medios en línea. El juez decide en 48 horas sobre esta petición. Hasta donde se ha podido conocer, no parece la medida muy efectiva, por cuanto sólo ha habido una decisión judicial[110], para no eliminar tweet de un Ministro.

Algunos fenómenos particulares como los «deepfakes» pueden merecer en el futuro una respuesta regulatoria, que podría circunscribirse al concreto ámbito electoral. Como se ha adelantado, Twitter por ejemplo ya adopta medidas al respecto (Twitter. s.f. a). Cabe ya mencionar la tibia regulación en la propuesta de Reglamento de Inteligencia artificial de la UE de 21 de abril 2021[111]. Su futuro artículo 52. 3.º impondrá hacer «público que el contenido ha sido generado de forma artificial», si bien no excluye que tales contenidos artificialmente falsos puedan estar amparados por la libertad de expresión.

Existen experiencias de regulación en EEUU especialmente para el ámbito electoral[112]. Así, en 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». 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». Se

110 Tribunal de Grande Instance de París, 17 de mayo de 2019, n ° 19/53935, https://www.dalloz-actualite.fr/document/tgi-paris-17-mai-2019-n-1953935

111 Comisión Europea, COM*(2021) 206 final, Propuesta de reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) de la UE*, 21 de abril 2021 https://eur-lex.europa.eu/legal-content/ES/TXT/DOC/?uri=CELEX:52021PC0206&from=ES

112 Vazquez, Lourdes. *Recommendations for Regulation of Deepfakes in the U.S.: Deepfake Laws Should Protect Everyone Not Only Public Figures*, 2020, https://www.ebglaw.com/wp-content/uploads/2021/08/Reif-Fellowship-2021-Essay-2-Recommendation-for-Deepfake-Law.pdf

trata de un ámbito novedoso respecto del cual cabe evaluar las experiencias regulatorias y sus posibles efectos políticos y en los concretos procesos electorales, así como en la libertad de expresión.

3. **Medidas y propuestas regulatorias respecto de la publicidad política**

Anteriormente se expusieron acciones de las principales redes sociales en materia de desinformación, obviamente aplicables en periodo electoral. Específicamente las plataformas han adoptado medidas respecto de la verificación de anunciantes, repositorios para investigadores y más funciones de supervisión, así como concretas funciones de información verificada y contextual.

En el ámbito de la publicidad política *Facebook*[113] tiene un sistema de verificación y autorización previa de anunciantes y desde la transparencia tienen una base de datos de anuncios[114]. También cuentan con sistemas para los usuarios que explican por qué ven determinados contenidos o anuncios, incluyendo la posibilidad de expresar preferencias. Entre las diversas medidas de *Google* se cuenta con un Informe de Transparencia de Anuncios Electorales[115] específico para la UE y una biblioteca de anuncios y un sistema de verificación de identidad de anunciantes. *Twitter*[116] desde 2019 directamente prohíbe en todo el mundo la publicidad política, según la han definido.

A este respecto, por cuanto a la normativa a adoptar, cabe partir de la jurisprudencia del TEDH y especialmente destaca la STEDH Animal Defenders International v. Reino Unido de 22 de abril 2013. En el ámbito de las prohibiciones de publicidad electoral, el tribunal parte de la falta de consenso europeo así como reconoce una importante discrecionalidad de los países al respecto. En esta sentencia el TEDH (n.º 120 y ss.) subraya la importancia que tienen las plataformas y redes sociales en el ámbito político. No obstante, entiende que no alcanza al impacto que tienen los medios masivos de difusión. Es por ello que el tribunal acepta que las prohibiciones de publicidad electoral se den sólo respecto de los medios masivos y no en plataformas.

Ahora bien, se trata de una cuestión en proceso de cambio. Más recientemente la Comisión de Venecia (principio 6.º) apuesta porque se revisen normas y reglamentos sobre publicidad política. Hasta la fecha, para una posible

113 Facebook, *Políticas de publicidad*, (sin fecha), https://www.facebook.com/policies/ads

114 Facebook, *Anuncios sobre temas sociales, elecciones o política*, (sin fecha), https://www.facebook.com/business/help/issuesandpolitics También, *Biblioteca de anuncios*. https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=ES&media_type=all

115 Google, *Informe de Transparencia. Publicidad política en la Unión Europea y en el Reino Unido,* (sin fecha), https://transparencyreport.google.com/political-ads/region/EU

116 Twitter, *Contenido de carácter político*, (sin fecha), https://business.twitter.com/es/help/ads-policies/ads-content-policies/political-content.html

regulación española se contaba como posible referente la propuesta irlandesa[117]. No obstante, la UE acaba de insistir en evitar cualquier fragmentación en la UE en todo lo que afecte a las plataformas. Para ello ha dado un paso importante para imponer bases comunes regulatorias. Así, el Código de Prácticas sobre Desinformación de 2018 ya establece que la publicidad política debe distinguirse claramente del contenido, un compromiso de revelar públicamente quién patrocina los anuncios y garantizar cierta transparencia. La propuesta de DSA incluye para las muy grandes plataformas obligaciones de repositorios de anuncios interoperables (arts. 30.2 y 34) pensados especialmente para la supervisión e investigación de anuncios y técnicas manipulativas de desinformación (Considerando 62). Una vez remitido este estudio, la Comisión ha presentado la propuesta de Reglamento UE sobre la transparencia y la focalización de la publicidad política, con 70 considerandos y 20 artículos[118]. El futuro Reglamento dedica un amplio capítulo (arts. 4-11) donde detalla todas las obligaciones a quienes preparan, promueven o difunden publicidad política. Especialmente hay que incentivar que las plataformas compartan datos relevantes y detallados para evaluar la eficacia de sus políticas publicitarias y la investigación incluso en tiempo real. Así, se dan obligaciones de transparencia, identificación de los servicios de publicidad política, registro y transmisión de información, requisitos de transparencia para cada anuncio político, información periódica sobre los servicios de publicidad política, indicación de anuncios políticos posiblemente ilegales, así como la transmisión de información a las autoridades competentes y a otras entidades interesadas. Los editores de la publicidad, como redes y plataformas) han de declarar como tal y etiquetar la publicidad política, indicar quién la paga, así como información clave de contexto (patrocinador, importe, fuentes de los fondos utilizados). La información debe transmitirse a las autoridades. Asimismo, están obligados a establecer mecanismos donde los ciudadanos puedan notificar el incumplimiento de las obligaciones.

Otro capítulo, muy vinculado a la protección de datos, regula obligaciones y prohibiciones respecto de las técnicas segmentación y amplificación políticas, con particularidades cuando se manejan datos sensibles. Quienes utilicen estas técnicas han de contar con políticas internas. Se exige el consentimiento expreso y también se permiten estas técnicas en el marco de los miembros de partidos, sindicatos y asociaciones. Se obligará a incluir información clara de porqué la publicidad política se dirige al concreto usuario, así como el deber de informar los

117 Department of the Taoiseach. Irlanda, *Online Political Advertising in Ireland: Regulation of Transparency*, febrero de 2019, recomendación 3 sobre publicidad política en línea de pago dentro de los períodos electorales https://www.gov.ie/en/policy-information/7a3a7b-overview-regulation-of-transparency-of-online-political-advertising-/

118 Comisión Europea, COM (2021) 731 final, *Proposal for a Regulation on the transparency and targeting of political advertising*, 25 de noviembre de 2021, https://ec.europa.eu/info/sites/default/files/2_1_177489_pol-ads_en.pdf

grupos de personas segmentados y los métodos de amplificación. Todo ello bajo el severo régimen sancionador del RGPD.

4. Necesarias concreciones de protección de datos para plataformas en el ámbito político y electoral

Desde la perspectiva de protección de datos, cabe recordar que la STC 76/2019, de 22 de mayo declaró inconstitucional la ley que permitía a los partidos políticos hacer perfilados políticos a partir del uso de redes sociales (artículo 58 bis de la Ley Orgánica 5/1985), especialmente por no haberse regulado con las suficientes garantías. Aunque aquello fue un motivo para congratularse, tal declaración de inconstitucionalidad no tuvo consecuencias prácticas. La atención no debería centrarse tanto en qué tratamientos de datos pueden hacer los partidos políticos, sino especialmente las plataformas y redes, que son a quienes partidos contratan sus servicios. Y ello pese a que, como se ha señalado, en teoría para la Junta Electoral los partidos sólo pueden contratar servicios para su uso de redes durante la campaña electoral.

Las campañas de desinformación estructuradas por lo general parten de una gestión muy avanzada de nuestros datos tanto por quienes las impulsan como por las plataformas y redes[119]. La Comisión de Venecia (2020, principio 4.º) ha recordado que «los datos personales deben protegerse de manera eficaz, especialmente durante el período crucial de elecciones». En esta materia, el RGPD y la Ley Orgánica 3/2018 deben concretarse y aclararse en no pocos aspectos para que sus mandatos se hagan efectivos. Hay que seguir especialmente las Directrices 8/2020 del Comité Europeo de Protección de Datos[120] sobre la orientación de los usuarios de las redes sociales. Sería muy conveniente que la AEPD estableciera instrucciones y lineamientos claros a seguir por las plataformas, redes y en su caso otros agentes implicados en el contexto electoral. Siguen resultando de interés los claros lineamientos de la Circular 1/2019 de la AEPD[121], pero hay que actualizarlos. La AEPD bien podría:

119 González de la Garza, L. M., *Redes sociales, instrumentos de participación democrática: análisis de las tecnologías implicadas y nuevas tendencias*, Dykinson, Madrid, 2015, del mismo autor, «La crisis de la democracia representativa. Nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el microtargeting y el Big Data», en *Revista De Derecho Político*, *1*(103), 2018, pp. 257-30, https://doi.org/10.5944/rdp.103.2018.23203; Castellanos Claramunt J., «La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos». *MÉI: Métodos de Información*, Vol. 11, n.º 21, 2020, pp. 42-58.

120 CEPD, Comité Europeo de Protección de Datos, *Guidelines 08/2020 on the targeting of social media users*, 7 de septiembre 2020. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-082020-targeting-social-media-users_en

121 AEPD, Agencia Española de Protección de Datos, *Circular 1/2019, de 7 de marzo, 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*, 2019, https://www.aepd.es/es/documento/boe-2019-3423.pdf

— determinar el régimen concreto que rige a plataformas y redes como encargados del tratamiento de datos por partidos y candidatos. Hay que aclarar también los responsables y corresponsables de los tratamientos de datos implicados.
— Respecto del consentimiento de los usuarios de redes, cabe determinar su posible invalidez por hacerse un uso desproporcionado de datos (art. 7.4.º RGPD). También habría de delimitarse la prohibición de tratar datos «cuya finalidad principal sea identificar su ideología, afiliación sindical, religión» (art. 9.1 Ley orgánica 3/2018 y art. 9.2.a) RGPD), esto es, casos en los que está prohibido tratar estos datos ideológicos incluso contando con el consentimiento de los usuarios.
— Establecer criterios sobre las configuraciones por defecto a aplicar por redes y plataformas a partir de los principios y obligaciones de protección de datos.
— Adoptar directrices claras sobre cuándo se considera que el usuario ha hecho manifiestamente públicos sus datos ideológicos o conexos en las redes, a los efectos de que se pudiera hacer tratamiento de los mismos (artículo 9.2.e) RGPD). Respecto del consentimiento debe tenerse en cuenta la doctrina restrictiva de la STC 27/2020, de 24 de febrero, que no va en la línea de permitir que se traten datos pese a que estén a la vista en redes y plataformas: «el usuario de Facebook que «sube», «cuelga» o, en suma, exhibe una imagen para que puedan observarla otros, tan solo consiente en ser observado en el lugar que él ha elegido (perfil,muro, etc.)» (FJ 2.º).
— Especificar los datos concretos que se pueden o no manejar en el contexto político electoral. En particular, se requerirían aclaraciones respecto de los datos que son especialmente protegidos (art. 9.2.º RGPD) por estar vinculados con la ideología. También que se esclareciera el régimen de los datos combinados de los usuarios que maneja la plataforma y que llevan a inferencias sobre la ideología. También debe concretarse qué tratamiento pueden hacerse sobre la posibilidad de tratamiento de los datos no aportados por los usuarios, sino los observados y los que las plataformas infieren de los ellos.
— En lo posible, debe determinarse la duración del tratamiento de los datos por plataformas. Y respecto de los tratamientos de datos concretos, cabe especificar la posibilidad de empleo de técnicas como el *microtargeting* o técnicas que puedan forzar o desviar la voluntad de los electores (art. 6 Circular 1/2019), ello, en la línea de la propuesta de Reglamento de noviembre 2021.
— En el marco de los derechos ya reconocidos de protección de datos, cabría articular mecanismos para que los usuarios de plataformas y redes puedan conocer y gestionar sus perfiles y preferencias respecto de la información y publicidad política que reciban.

— El artículo 23 Ley Orgánica 3/2018 sobre sistemas de exclusión publicitaria debe concretarse para aclarar los términos y facilitar la implantación efectiva de la posibilidad de *listas Robinson* para el ámbito electoral, por las que voluntariamente los usuarios de redes puedan excluir el tratamiento de sus datos en las plataformas y redes para usos políticos y electorales.
— También para el ámbito político deben especificarse las medidas de seguridad obligatorias a adoptar, las técnicas de anonimización y seudonimización de los datos, así como especificaciones respecto de los registros de actividades y estudios de impacto de tratamiento de datos (art. 35.4.º RGPD). Igualmente, las pautas concretas de actuación frente a brechas de seguridad
— Debe fijarse la transparencia e información obligatoria concreta a suministrar por plataformas, redes y en su caso sujetos implicados. De especial interés es la determinación de la procedencia de los datos y las comunicaciones previstas de los mismos. También caben especificaciones sobre elementos técnicos de la interfaz a través de la cual facilitar los datos y la posible conexión con el derecho a la portabilidad.
— En tanto en cuanto las redes y plataformas utilizan técnicas sólo automatizadas, debe fijarse la aplicabilidad del artículo 23 RGPD y la posibilidad de una especial transparencia y explicabilidad de la lógica de los algoritmos utilizados.

XI. CONCLUSIONES: CONSTITUCIONALMENTE, POCO SE PUEDE HACER, PERO QUEDA MUCHO POR HACER

Que la desinformación es una enfermedad para la democracia, sin duda; que los remedios pueden ser aún peor que la enfermedad, también. Si se quiere lograr algo positivo, hay que ser humildes y posibilistas. Se ha partir de que en la lucha constitucional contra la desinformación hay que hacerla con el *freno echado*, amén de que es una lucha posiblemente perdida. Hay que aceptar que en democracia no hay una verdad; que el riesgo de que los poderes públicos intenten imponer, o sólo orquestar u orientar hacia una verdad es peor que la enfermedad de la desinformación. Hay que asumir que el único concepto de desinformación sobre el que constitucionalmente se puede actuar, ya de inicio es tan restringido que deja fuera muchos desórdenes de la información sobre los que no se puede actuar. Y posiblemente los más importantes.

También hay que partir de que ya sólo monitorear e identificar la «desinformación» puede ser peligroso. Que es necesario determinar qué autoridades, con qué independencia y cómo lo harán, así como fijar elementos de transparencia y las posibilidades de control. Si controlar contenidos es sensible, tampoco puede confiarse totalmente en los sistemas automáticos que detectan las conductas o pautas de actuación de los propagadores de desinformación. No olvidemos que

estos sistemas, por asépticos que puedan parecer, pueden llevar a la masiva desactivación de contenidos sin conocimiento ni garantía alguna. Especialmente si interviene el Gobierno, hay que estar muy alerta ante cualquier control de contenidos, o frente a las acciones que escondan eufemismos como «minimizar» los efectos de la desinformación, recordando la utilizada por el Jefe de Estado Mayor de la Guardia Civil en 2020.

En la lucha frente a la desinformación también hay que aceptar que no habrá prácticamente instrumentos legales mundiales: a los sistemas no democráticos la desinformación les afecta muy poco y, además, les sirve como excusa para reforzar su soberanía y control sobre su Internet y para reprimir el discurso político contrario al Gobierno. Y otra barrera: si se quiere luchar contra la desinformación, tampoco se puede regular la cuestión *por las bravas* en la arena nacional (como Alemania o Francia, o proyectos como Polonia). Todo lo que se haga necesariamente ha de partir del marco de la UE, evitando cualquier fragmentación que perjudicaría no sólo a los intereses de las grandes plataformas, sino a las bases sobre las que fluyen las libertades informativas en el siglo XXI. Y bueno, en esta relación de lo que hay que asumir o no se debe hacer, por supuesto que no se pueden adoptar decisiones como el decretazo digital (Real Decreto-Ley 14/2019), que deja a la discrecionalidad y opacidad del Gobierno la intervención y control de Internet y sus operadores sin garantías.

Pero entonces, ¿se puede hacer y regular algo? Como se ha analizado, sí y mucho. De hecho, las plataformas afortunadamente ya lo hacen. Pero con escaso o nulo marco jurídico y no siempre buscando los mismos objetivos que los Estados, ni la defensa de los derechos de los millones de sus usuarios. También son muchas las acciones iniciadas en el ámbito de la UE, como el Código de Buenas Prácticas de 2018, sus planes de acción o el *Rapid Alert System* (RAS).

Destaca especialmente la futura DSA —ley de servicios digitales—, su acertado modelo de corregulación delimita el alcance de las libertades de empresa e informativas de las plataformas. Este modelo también permite al Estado velar por los intereses públicos en juego y, especialmente, garantizar las libertades informativas de cientos de millones de usuarios de las redes. Así, la regulación propuesta parte de las acciones y autorregulaciones ya adoptadas por las plataformas contra la desinformación y las reorienta e impulsa hacia los objetivos necesarios. El control, rastreo, moderación, restricción, mayor o menor visibilidad de unos u otros contenidos, en muchos casos a través de algoritmos, dejan de estar bajo la total discrecionalidad de las plataformas. Sus poderes de decisión sobre los contenidos deben quedar bajo la posible supervisión, así como contar con transparencia y garantías de debido proceso. Pese a que la música es buena, habrá que esperar a la letra definitiva.

Y la concreción normativa no sólo depende de la futura DSA, sino también de los desarrollos regulatorios nacionales: determinación de las autoridades competentes y su independencia, facultades, así como la fijación de las garantías y derechos efectivos de los usuarios. En el nivel nacional se han detectado palos

de ciego, al tiempo de apreciarse algunos peligrosos tics para la libertad de expresión. Se ha iniciado un razonable primer paso con la Orden PCM/1030/2020, de 30 de octubre, que ha levantado más polvareda que otra cosa. Aquí se han señalado algunos elementos que ha de seguir la regulación de la gobernanza en la materia, algo necesario. También en el plano nacional hay margen regulatorio para el fomento del periodismo, la alfabetización y educación contra la desinformación, así como se pueden detallar garantías respecto de la actuación de los verificadores de noticias o fact-checkers u otros agentes que actúen contra la desinformación.

La UE ha asumido también la iniciativa regulatoria en el ámbito electoral. El 25 de noviembre de 2021 se ha presentado la propuesta de Reglamento UE sobre publicidad política, con importantes obligaciones para anunciantes y plataformas, de especial incidencia también en materia de protección de datos. Pues bien, la capacidad regulatoria en España es importante. En el ámbito de protección de datos el TC ya mostró sensibilidad en su STC 76/2019, de 22 de mayo y siendo necesaria la regulación de garantías suficientes. Aquí se han enunciado. Por cuanto al terreno electoral aún son mayores las posibilidades de regulación. La misma Junta Electoral ha tenido recordar en su Acuerdo 146/2021 que hay que regular mejor sus competencias y capacidades especialmente respecto de las plataformas, así como las garantías de los sujetos electorales. Poco se puede hacer, pero queda mucho por hacer.

Bueno, se podía pensar que poco se podía hacer hasta la invasión de Ucrania en febrero 2022. Sin embargo, la UE ha actuado por las bravas ordenando del cierre de canales rusos en internet por ser propaganda desinformativa, como se ha detallado. Ello supone un punto de inflexión. Considero que han saltado por los aires no pocos resortes y garantías que aquí se han expuesto. Lo más peligroso a mi juicio es la escasa o más bien nula reacción frente a estas medidas, ni desde la sociedad civil, ni desde los juristas. Se trata de un negativo precedente que abre con fuerza una puerta, la de futuras y graves restricciones de las libertades informativas en razón —o con la excusa— de la desinformación y propaganda. Esperemos que no sea así.

***

TITLE: *Who, how and what to regulate (or not regulate) against disinformation*

ABSTRACT: *The regulatory response to disinformation is complex, both in terms of who and how should do it, and because the freedom of expression and information of users and also of networks and platforms are at stake. Many disinformation phenomena that are to be prevented must be left out of the legal response. In many areas it is best not to regulate, and it is also necessary to prevent non-independent governmental bodies from assessing or restricting content and from being able to orchestrate political debate. The European Union sets the regulatory framework. Networks and platforms and states regulate on the basis of this EU framework. Policies, Code of Practice and the future Digital Services Act are examined; also the international regulation of disinformation as undue influence operations. Self-regulatory or co-regulatory models such as the future DSA are positively considered. This model would channel and drive the current efforts of networks and*

platforms. The lines of (self-)regulation of fack cheeckers are also formulated. In the specific Spanish context, regulatory attempts are described. The information security regulation applicable to disinformation is opaque and needs to be clarified. It is also stated that the "decretazo digital" of 2019 is unconstitutional. Also, the controversial Order of 2020 is analyzed and possible improvements are pointed out. Finally, some comparative regulations for the electoral field (on influence operations, judicial removal of content or deepfakes) are taken into account. Specific proposals are made to regulate the electoral regime, also regarding political advertising and data protection for platforms.

Resumen: *La respuesta regulatoria frente a la desinformación es compleja tanto por quiénes y cómo deben realizarla, cuanto porque están en juego las libertades de expresión e información de usuarios y también de redes y plataformas. Hay que asumir que muchos fenómenos de desinformación que se quieren evitar tendrán que quedar fuera de la respuesta jurídica. Se afirma que en muchos ámbitos lo mejor es no regular o que hay que evitar que órganos gubernamentales no independientes evalúen o restrinjan los contenidos y puedan orquestar debate político. La Unión Europea establece el marco regulatorio y a partir del mismo actúan y regulan tanto las redes y plataformas cuanto los Estados. Se examinan las políticas, Código de buenas prácticas, futura Digital Services Act y la regulación internacional de la desinformación como operaciones de influencia indebidas. Se consideran positivos los modelos de autorregulación o corregulación como la futura DSA, que puede encauzar e impulsar los actuales esfuerzos voluntarios de las redes y plataformas. También se formulan las líneas de (auto)regulación de la verificación de noticias. En el ámbito concreto español, se describen las inercias que ha habido, la necesidad de mejorar la opaca regulación española de la seguridad de la información aplicable, así como el inconstitucional «decretazo digital». En especial, se analiza la polémica Orden de 2020 y se señalan posibles mejoras de la regulación institucional y orgánica de la desinformación. Finalmente, se tienen en cuenta algunas regulaciones comparadas para el ámbito electoral (sobre operaciones de influencia, retirada judicial de contenidos o deepfakes). Se formulan concretas propuestas de regulación del régimen electoral, también respecto de la publicidad política y protección de datos para plataformas.*

Key words: *disinformation, freedom of expression, journalism, social networks, Internet, electoral law, self-regulation, European Union, data protection, fack cheeckers.*

Palabras clave: *desinformación, libertad de expresión, periodismo, redes sociales, Internet, Derecho electoral, autorregulación, Unión Europea, protección de datos, verificadores.*

Fecha de recepción: *09.12.2021* Fecha de aceptación: *02.02.2022*