

Isabel Serrano Maíllo  
Loreto Corredoira  
(Editoras)



# DEMOCRACIA Y DESINFORMACIÓN

Nuevas formas de polarización,  
discursos de odio y campañas en redes.  
Respuestas regulatorias de Europa y América Latina

A central illustration of a globe surrounded by various elements: books, hot air balloons, and a city skyline. The globe is the central focus, with books floating around it, some open and some closed. Hot air balloons are scattered throughout the scene, and a city skyline is visible in the background. The overall color palette is dominated by blues and greens, with a white cloud-like base.

*Dykinson, S.L.*



# DEMOCRACIA Y DESINFORMACIÓN

NUEVAS FORMAS DE POLARIZACIÓN, DISCURSOS DE  
ODIO Y CAMPAÑAS EN REDES. RESPUESTAS REGULATORIAS  
DE EUROPA Y AMÉRICA LATINA



# DEMOCRACIA Y DESINFORMACIÓN

NUEVAS FORMAS DE POLARIZACIÓN, DISCURSOS DE  
ODIO Y CAMPAÑAS EN REDES. RESPUESTAS REGULATORIAS  
DE EUROPA Y AMÉRICA LATINA

Isabel Serrano Maíllo

Loreto Corredoira

**(Editoras)**

Pedro Anguita	Oscar Jaramillo Castro
Vitor de Andrade Monteiro	María José Labrador Blanes
Tamara Antona Jimeno	Ana Mayagoitia-Soria
Ferran Armengol Ferrer	Adrián Merinero Sánchez
Altus Alejandro Baquero Rueda	José Javier Olivas Osuna
Javier Barriuso Bernad	María Antonia Paz Rebollo
Ignacio Bel	Florentino Portero
Rodrigo Cetina Presuel	Rafael Rubio Núñez
Mariluz Congosto Martínez	José Manuel Saavedra Molina
Loreto Corredoira	Francisco Segado Boj
Yevhen Fedchenko	Isabel Serrano Maíllo
Rocío Gómez	Nairbis Desiree Sibrian Díaz
Juan Manuel Gozález Aguilar	Mireya Vincent-Ibáñez
Miguel Ángel Gonzalo	Jessica Zorogastua Camacho
Alejandra Jans	

*Dykinson, S.L.*

No está permitida la reproducción total o parcial de este libro, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio, sea éste electrónico, mecánico, por fotocopia, por grabación u otros métodos, sin el permiso previo y por escrito del editor. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (art. 270 y siguientes del Código Penal).

Diríjase a Cedro (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra. Puede contactar con Cedro a través de la web [www.conlicencia.com](http://www.conlicencia.com) o por teléfono en el 917021970/932720407

Este libro ha sido sometido a evaluación por parte de nuestro Consejo Editorial

Para mayor información, véase [www.dykinson.com/quienes\\_somos](http://www.dykinson.com/quienes_somos)

©Copyright by los autores

Madrid, 2024

“Publicado en el marco del Proyecto de Investigación “Dir-Politics. Garantías institucionales y regulatorias. Autoridades electorales y de supervisión digital ante interferencias, narrativas hostiles, publicidad segmentada y polarización”. Financiado por el Ministerio de Ciencia e Innovación. Referencia PID2022-137245OB-I00”.

Patrocinan:



Editorial DYKINSON, S.L.

Meléndez Valdés, 61 - 28015 Madrid

Teléfono (+34) 915442846 - (+34) 915442869

e-mail: [info@dykinson.com](mailto:info@dykinson.com)

<http://www.dykinson.es>

<http://www.dykinson.com>

ISBN: 978-84-1170-948-4

Depósito Legal: M-9020-2024

DOI: 10.14679/2616

ISBN electrónico: 978-84-1070-284-4

*En memoria de todos los profesionales del periodismo que han arriesgado sus vidas para hacer posible el derecho universal a la información del artículo 19 DUDH.*

En Madrid, 10 de diciembre de 2023,  
45° Aniversario de la Declaración Universal de Derechos Humanos.



# ÍNDICE

PRÓLOGO..... 13  
*Carmen Romero*

## PARTE I. INTRODUCCIÓN

VISIÓN GLOBAL DE LAS AMENAZAS INTERNACIONALES EN  
CIBERSEGURIDAD ..... 19  
*Florentino Portero*

LIBERTAD, ÉTICA Y VERDAD, SOLUCIONES FRENTE A LA  
DESINFORMACIÓN..... 37  
*Ignacio Bel*

## PARTE II. CALIDAD DE LA DEMOCRACIA, SEGURIDAD Y COOPERACIÓN. INVESTIGACIONES SOBRE INTERFERENCIAS ELECTORALES Y DEMOCRACIA. INVESTIGACIÓN ACADÉMICA Y DE MEDIOS

DESINFORMACIÓN COMO BURLA: LOS MEMES POLÍTICOS.  
UN CASO DE ESTUDIO ..... 53  
*María Antonia Paz Rebollo, Ana Mayagoitia-Soria y  
Juan Manuel González-Aguilar*

DESINFORMACIÓN E INSTRUMENTALIZACIÓN DE INSTITUCIONES ACADÉMICAS, POLÍTICAS Y PRENSA: EL CASO CATALANGATE .....	71
---	----

*José Javier Olivas*

ACTIVISMO, DESINFORMACIÓN Y CAMPAÑAS EN REDES. ESTUDIO DE TWITTER, TELEGRAM Y TIKTOK.....	93
---	----

*Mariluz Congosto Martínez y Javier Barriuso Bernad*

CARACTERIZACIÓN DEL FLUJO INFORMATIVO DE LA DESINFORMACIÓN EN REDES SOCIALES: EL CASO CHILENO EN TWITTER ENTRE 2018 Y 2022.....	121
---	-----

*Oscar Jaramillo*

DESINFORMACIÓN Y MARCOS REGULATORIOS EN AMÉRICA LATINA: DESAFÍOS EN TORNO A DISCURSOS DE ODIO, ELIMINACIÓN MASIVA DE DATOS Y DERECHO AL OLVIDO.....	139
---	-----

*Nairbis Sibrian y María José Labrador*

ANÁLISIS EXPLORATORIO SOBRE LOS FACTORES QUE INFLUYEN EN LA DISEMINACIÓN DE NOTICIAS FALSAS QUE CONTIENEN DISCURSOS DE ODIO .....	163
---	-----

*Tamara Antona-Jimeno, Mireya Vicent-Ibáñez, Francisco Segado-Boj y Adrián Merinero-Sánchez*

PREOCUPACIONES Y VISIÓN DE LA INVASIÓN DE UCRANIA DESDE EL SUR GLOBAL .....	181
---	-----

*Yevhen Fedchenko*

FRAGMENTACIÓN TRAS 25 AÑOS DE PACIFICACIÓN DEL PERÚ: POLARIZACIÓN INFORMATIVA, POLÍTICA Y SOCIAL .....	197
--	-----

*Jessica Zorogastua Camacho y Jose Manuel Saavedra Molina*

**PARTE III.**  
**RESPUESTAS REGULATORIAS LATAM-EUROPA.**  
**POLÍTICAS PÚBLICAS Y GARANTÍAS REGULATORIAS**

INTERFERENCIAS EXTRANJERAS EN LOS ESTADOS DEMOCRÁTICOS. ANÁLISIS DE LOS INFORMES DEL PARLAMENTO EUROPEO Y LAS ASAMBLEAS PARLAMENTARIAS DE LA OTAN Y DEL CONSEJO DE EUROPA.....213

*Miguel Ángel Gonzalo*

EL DELITO DE ODIOS: ¿UN NUEVO LÍMITE DESPROPORCIONADO E INJUSTO A LA LIBERTAD DE EXPRESIÓN?..... 231

*Isabel Serrano Maíllo*

ALERTADORES FIABLES: DE SU CODIFICACIÓN EN LA DSA A LA NECESIDAD DE ATENDER SUS LIMITACIONES .....251

*Rodrigo Cetina Presuel*

DEMOCRACIA Y DESINFORMACIÓN. RESPUESTAS REGULATORIAS DE LA UNIÓN EUROPEA PARA EL FORTALECIMIENTO DE LA DEMOCRACIA Y CAMBIOS DE RUMBO DEL PAQUETE DE SERVICIOS DIGITALES .....267

*Loreto Corredoira*

LIBERTAD DE EXPRESIÓN, PROPAGANDA ELECTORAL Y REDES SOCIALES (COLOMBIA).....295

*Altus Alejandro Baquero Rueda*

COMISIÓN ASESORA CONTRA LA DESINFORMACIÓN: PRIMERA ACCIÓN DEL GOBIERNO DE CHILE PARA COMPRENDER LOS TRASTORNOS DE LA COMUNICACIÓN .....311

*Pedro Anguita, Rocío Gómez y Alejandra Jans*

LA ACTUACIÓN NO JURISDICCIONAL DEL ÓRGANO ELECTORAL BRASILEÑO FRENTE A LA DESINFORMACIÓN.....	327
---	-----

*Rafael Rubio Núñez y Vitor de Andrade Monteiro*

DESINFORMACIÓN EN LA UNIÓN EUROPEA: DE LA GUERRA HÍBRIDA AL ESPACIO EUROPEO DE LA LIBERTAD DE INFORMACIÓN.....	345
--	-----

*Ferran Armengol Ferrer*

# **INTERFERENCIAS EXTRANJERAS EN LOS ESTADOS DEMOCRÁTICOS. ANÁLISIS DE LOS INFORMES DEL PARLAMENTO EUROPEO Y LAS ASAMBLEAS PARLAMENTARIAS DE LA OTAN Y DEL CONSEJO DE EUROPA**

MIGUEL ÁNGEL GONZALO

*Documentalista (Congreso de los Diputados). Profesor asociado (UCM)*

## **Sumario:**

1. INTRODUCCIÓN

2. MARCO TEÓRICO

**2.1 Evolución histórica de la interferencia extranjera**

*2.1.1 Periodo pre-digital*

*2.1.2 Era digital*

**2.2 Teorías y conceptos clave relacionados con la interferencia extranjera y la desinformación**

*2.2.1 Teorías del Realismo en Relaciones Internacionales*

*2.2.2 Teoría de la Información Asimétrica*

**2.3 Ciberseguridad**

3. EL TRABAJO DE LA COMISIÓN EUROPEA

4. ANÁLISIS DE LOS INFORMES DEL PARLAMENTO EUROPEO

5. LEY DE SERVICIOS DIGITALES

6. ASAMBLEA PARLAMENTARIA DE LA OTAN

7. ANÁLISIS DE LOS INFORMES DEL CONSEJO DE EUROPA

8. CONCLUSIÓN

9. BIBLIOGRAFÍA UTILIZADA

*“En tiempos de engaño universal, decir la verdad se convierte en un acto revolucionario”.*

George Orwell

*“La única seguridad de todo está en una prensa libre. La fuerza de la opinión pública es irresistible cuando se le permite expresarse libremente”.*

Thomas Jefferson

## 1. INTRODUCCIÓN

En el tablero político global, la soberanía y autonomía de los estados democráticos representan pilares esenciales para la salvaguarda de los valores democráticos y el ejercicio pleno de los derechos y libertades de la ciudadanía. Sin embargo, la era de la globalización y la revolución digital han generado un nuevo territorio en el que las fronteras nacionales parecen cada vez más permeables, incluso híbridas, especialmente en el ámbito de la información y comunicación. Es en este contexto de interconexión donde surge con vigor renovado el fenómeno de la interferencia extranjera, entendida como la intrusión no deseada o intromisión de un estado o actor extranjero en los asuntos internos de otro estado, con el objetivo de influir en decisiones políticas, procesos electorales, o la opinión pública. La Interferencia Extranjera y Manipulación de la Información (FIMI, por sus siglas en inglés) describe un patrón de comportamiento en su mayoría no ilegal, aunque lógicamente puede tener componentes delictivos, que amenaza o tiene el potencial de afectar negativamente los valores, los procedimientos y el proceso político. Dicha actividad es de carácter manipulador, realizada de manera intencional y coordinada por actores estatales o no estatales, incluidos sus representantes dentro y fuera de su propio territorio. La interferencia extranjera no es un fenómeno reciente; ha acompañado las relaciones internacionales desde siempre. Sin embargo, la era digital ha proporcionado nuevas herramientas y métodos para efectuarla, ampliando su alcance y potencial impacto. Las tácticas empleadas van desde la propagación de desinformación y discursos de odio, hasta ciberataques dirigidos y financiamiento ilícito de campañas políticas. Estas acciones, meticulosamente orquestadas, buscan en muchos casos exacerbar tensiones sociales, desestabilizar gobiernos, y socavar la confianza en las instituciones democráticas. Sin embargo, al igual que cuando se analiza el concepto de desinformación es necesario superar la clásica dicotomía entre verdad y mentira, cuando se analiza la FIMI también hay que abrir el foco de análisis para superar enfoques del pasado. La relevancia de este tema que se aborda en este libro radica en su potencial para

amenazar la integridad y estabilidad de las democracias. Los estados democráticos, con sus principios de origen liberal tales como la libertad de expresión y participación ciudadana, por ejemplo, pueden ser, y de hecho lo son, especialmente vulnerables a estas tácticas de interferencia. Las campañas de desinformación, por ejemplo, pueden polarizar a la sociedad, fomentando divisiones y hostilidades. Los ciberataques a infraestructuras críticas pueden tener consecuencias devastadoras, afectando la vida cotidiana de la ciudadanía y convirtiéndose en asuntos de seguridad nacional. Además, la interferencia extranjera puede erosionar la confianza en las instituciones democráticas y en el proceso electoral, elementos cruciales para el funcionamiento adecuado de cualquier democracia asentada. El objetivo principal de este capítulo es explorar y analizar los informes relevantes de organismos de la Unión Europea como la Comisión o el Parlamento Europeo, así como de las asambleas parlamentarias de organismos como la OTAN o el Consejo de Europa en relación con la interferencia extranjera en los estados democráticos. Estos informes representan esfuerzos significativos a nivel supranacional para comprender, documentar y proponer soluciones a este creciente desafío. A través del análisis de estos informes, se busca identificar las principales preocupaciones, recomendaciones y estrategias propuestas por estas instituciones europeas para contrarrestar la interferencia extranjera, y evaluar su aplicabilidad y efectividad potencial. Al entender las dimensiones de la interferencia extranjera y las propuestas institucionales para mitigarla, este capítulo aspira a contribuir al diálogo y la formulación de políticas necesarias para proteger y fortalecer las democracias frente a las amenazas externas en el siglo XXI. Además, se propone fomentar una discusión informada sobre cómo los estados democráticos pueden, a través de la cooperación interparlamentaria regional e internacional, forjar estrategias efectivas para mitigar los riesgos asociados con la interferencia extranjera y, en última instancia, preservar los valores y principios democráticos que forman la base de nuestras sociedades, como se ha dicho anteriormente.

## 2. MARCO TEÓRICO

### 2.1. Evolución histórica de la interferencia extranjera

#### 2.1.1. *Periodo pre-digital*

No es el objetivo de este trabajo analizar el pasado, pero sí es necesario hacer una alusión a como en la era predigital el trabajo de influencia entre reinos o naciones ha estado presente en la geopolítica y cómo las potencias extranjeras han intentado in-

fluir en las monarquías y gobiernos a lo largo de la historia, por ejemplo, mediante matrimonios reales, alianzas políticas, o apoyo a facciones rivales. A título de mero ejemplo cercano se puede citar como en 1469, Isabel I de Castilla y Fernando II de Aragón contrajeron matrimonio, uniendo así dos de los reinos más poderosos de la península ibérica. Este matrimonio no solo tuvo implicancias significativas para la península, sino también para otras potencias europeas. Francia, que había disfrutado de la desunión de los reinos ibéricos, vio amenazada su posición de poder en Europa con la formación de esta unión dinástica, lo cual cambió el equilibrio de poder en el continente. Todo este proceso estuvo lógicamente plagado de acciones diplomáticas de influencia. Casos de alianzas políticas hay numerosísimos a lo largo de la historia, se puede citar meramente a título de ejemplo como, durante la Guerra de las Dos Rosas en Inglaterra (1455-1487), diversas potencias europeas proporcionaron apoyo a las casas rivales de Lancaster y York. Francia, por ejemplo, apoyó inicialmente a la Casa de Lancaster, mientras que la Casa de York recibió apoyo de Borgoña. Este apoyo extranjero no sólo prolongó el conflicto, sino que también influyó en el curso de la guerra y en el destino de la monarquía inglesa.

### *2.1.2. Era Digital*

Ya en la era digital cabe hacer alguna breve referencia a la influencia en las elecciones. Citemos el referente de la interferencia en las elecciones de EE.UU. de 2016. Una de las tácticas implicadas fue el hackeo y la posterior filtración de correos electrónicos de la campaña demócrata, lo que creó controversia y afectó la percepción pública de los candidatos. Este incidente destacó la necesidad de proteger la información sensible relacionada con las elecciones y reforzar la seguridad de las infraestructuras digitales relacionadas con los procesos electorales. Otro caso célebre fue el ataque al Servicio Nacional de Salud del Reino Unido de 2017. El ataque de ransomware conocido como WannaCry afectó a organizaciones en todo el mundo, incluido al citado organismo. Aunque no fue un acto de interferencia política per se, demostró cómo los actores malintencionados podrían afectar infraestructuras críticas de un país, causando caos y pérdidas económicas. La seguridad de los sistemas de información de infraestructuras vitales es esencial para la resiliencia y seguridad nacional. Durante las elecciones presidenciales de Francia en 2017, hubo un intento de influir en el electorado mediante la filtración de documentos relacionados con uno de los candidatos poco antes de la votación. Unos 14.5 gigabytes de emails y documentos personales y de negocios fueron publicados en el sitio web para compartir textos Pastebin por medio de enlaces a más de 70.000 archivos. Trabajadores del partido de Macron, ¡En Marche!, dijeron en un comunicado que los perpetradores del hackeo habían mezclado documentos falsos con auténticos “para crear confusión y desinfor-

mación”. Los estados deben estar preparados para identificar y contrarrestar tácticas de desinformación y filtración de documentos en tiempo real durante eventos críticos como las elecciones.

## **2.2. Teorías y conceptos clave relacionados con la interferencia extranjera y la desinformación**

La comprensión de las operaciones FIMI necesita una aproximación, siquiera sea somera, a las teorías que explican las injerencias extranjeras desde el punto de vista de la geopolítica.

La geopolítica en el siglo XXI se ha reafirmado como una disciplina clave para desentrañar la complejidad de un mundo cada vez más interconectado y, a la vez, fraccionado. Entender la geopolítica hoy en día es crucial para descifrar los eventos y tensiones que definen el orden mundial, ya que permite interpretar no solo las relaciones entre naciones, sino también cómo factores como el acceso a recursos, estrategias de seguridad nacional, y cambios en el balance global de poder afectan dichas dinámicas.

En este contexto, la geopolítica ilumina la comprensión de problemas transnacionales como el cambio climático, las pandemias y la ciberseguridad, demostrando que las soluciones a estos desafíos contemporáneos requieren un análisis que trascienda las fronteras nacionales.

En este capítulo describimos dos teorías básicamente complementarias, la teoría del realismo y la teoría de la información asimétrica.

### *2.2.1. Teorías del Realismo en Relaciones Internacionales*

Se trata de una teoría que explica las acciones de los países principalmente a través del prisma del poder. En un lenguaje más sencillo, el realismo sugiere que cada país actúa principalmente en su propio interés, buscando aumentar su poder y seguridad frente a otros países. Cuando hablamos de interferencia extranjera, esto puede verse como una extensión de este juego de poder. Bajo la óptica realista, las naciones interfieren en los asuntos internos de otras naciones con el objetivo principal de incrementar su propia influencia y poder, mientras debilitan a sus rivales. Durante la Guerra Fría, Estados Unidos y la Unión Soviética eran los dos “jugadores” principales. Ambos utilizaron técnicas de interferencia extranjera para ganar influencia. Por ejemplo, en varios países de América Latina, África y Asia, estas superpotencias apoyaron a facciones políticas y movimientos rebeldes que alineaban con sus respectivos intereses, no necesariamente porque se preocuparan por el bienestar de esos países, sino para expandir su esfera de influencia y poder.

### *2.2.2. Teoría de la Información Asimétrica*

Se refiere a situaciones donde un participante tiene más o mejor información que otro. En contextos internacionales, esta asimetría puede ser explotada por actores (países, grupos) para influir o manipular situaciones en otros estados. En un juego de cartas donde solo un jugador puede ver todas las cartas sobre la mesa mientras los demás no pueden. Ese jugador con “información privilegiada” tiene una ventaja significativa y puede usarla para ganar el juego. En el gran mercado de la información, diferentes actores (ciudadanos, gobierno, medios) compran y venden información. Ahora, si un actor extranjero tiene información que otros no tienen (o puede crear o distorsionar información), puede influir en las decisiones y percepciones dentro de ese país. En el contexto de elecciones, un país extranjero podría tener información detallada sobre los votantes de otro país (por ejemplo, sus preferencias, miedos, creencias). Este país extranjero podría usar esta información para crear campañas de desinformación altamente efectivas en redes sociales, dirigidas específicamente a ciertos grupos de votantes. Al hacerlo, podrían influir en la opinión pública, fomentando divisiones, desconfianza o apoyo a ciertos candidatos, sin que los votantes sean conscientes de que están siendo manipulados.

## **2.3 Ciberseguridad**

El concepto de ciberseguridad, entendida como un conjunto de tecnologías, procesos y prácticas diseñadas para proteger sistemas, redes y datos de ataques cibernéticos, en el contexto de interferencia extranjera, es crucial porque los estados necesitan proteger su información y sistemas de comunicación para preservar su soberanía, seguridad y el buen funcionamiento de sus instituciones democráticas. Todo ello por varias razones: en primer lugar, por la protección de Información sensible ya que los estados poseen información confidencial que, si se expone, podría ser utilizada por actores extranjeros para influir en decisiones políticas o desestabilizar el gobierno (Rid, T., & Fontal, Y., 2021); en segundo lugar, la preservación de la integridad electoral, dado que con los procesos electorales cada vez más digitalizados, garantizar un proceso electoral seguro y confiable es esencial para mantener la confianza en los resultados y las instituciones democráticas y, por último, como defensa contra la desinformación ya que cabe concluir que una ciberseguridad robusta puede identificar y neutralizar campañas de desinformación lanzadas por actores extranjeros en plataformas digitales y redes sociales. La ciberseguridad y la desinformación están intrínsecamente vinculadas en el panorama digital actual. Las vulnerabilidades de seguridad a menudo dan paso a la desinformación como un vector de ataque, donde actores con malas intenciones uti-

lizan información falsa o engañosa para sembrar confusión y pánico en la sociedad, facilitando otros ataques cibernéticos más directos. Estos actores, ya sean estatales o no estatales, aprovechan la manipulación de la opinión pública a través de campañas de influencia maliciosa. Estas campañas son meticulosamente diseñadas para crear y difundir contenido falso o engañoso con el objetivo de manipular la percepción pública, desacreditar a instituciones o individuos destacados y minar la confianza en procesos democráticos esenciales, como las elecciones.

Para enfrentar estos desafíos, es esencial adoptar respuestas y estrategias de mitigación efectivas. Tanto la lucha contra la desinformación como la promoción de la ciberseguridad se basan en herramientas y estrategias compartidas. Estas incluyen educar y concienciar al público, lo que implica fomentar una alfabetización digital y mediática robusta, la verificación constante de hechos y el empleo de tecnologías avanzadas para detectar y contrarrestar amenazas. Además, se necesitan estrategias interdisciplinarias (Wardle, C., Derakhshan, H., & Council of Europe. (2017, p. 78) que pongan en relación la cooperación internacional entre gobiernos, el sector privado y la sociedad civil es crucial, permitiendo compartir información vital y adoptar las mejores prácticas para garantizar un ciberespacio más seguro y veraz.

### 3. EL TRABAJO DE LA COMISIÓN EUROPEA

Dentro de este marco teórico a partir de aquí se pone el foco en el análisis y valoración de cómo la Unión Europea y la dimensión parlamentaria de organismos internacionales tan relevantes como la Organización del Tratado del Atlántico Norte y el Consejo de Europa están afrontando la lucha contra los desórdenes informativos derivados de las injerencias extranjeras. Hay que recordar que el parlamento español mantiene delegaciones permanentes en las asambleas de estos organismos lo que supone una muestra de la importancia de la colaboración interparlamentaria. Así pues, la proliferación de campañas de desinformación a gran escala representa uno de los desafíos más significativos que enfrenta Europa en la era digital. Para abordar este problema, es esencial una colaboración sin precedentes entre los países miembros de la UE, sus instituciones, las plataformas digitales, medios de comunicación y, por supuesto, la ciudadanía.

Entre las iniciativas clave que la UE ha emprendido en este ámbito, destaca la “Comunicación sobre la Lucha contra la Desinformación en Línea de 2018” (Comisión Europea, 2018) que expuso una serie de desafíos, implicaciones y propuestas para abordar esta problemática. La desinformación, entendida como la difusión de información engañosa o falsa, ha encontrado en Internet y las redes sociales un vehículo eficaz para alcanzar a grandes masas de población en tiempos récord. Esta realidad

plantea un desafío significativo para Europa, dado que la desinformación puede erosionar la confianza en las instituciones y medios de comunicación, obstaculizar la capacidad de los ciudadanos para tomar decisiones informadas y respaldar ideas y actividades radicales y extremistas. La emergencia de la era digital ha transformado la forma en que los ciudadanos acceden e interactúan con la información. Internet ha incrementado el volumen y diversidad de las noticias disponibles, mientras que las redes sociales y nuevas tecnologías han facilitado la difusión de desinformación a una escala y velocidad sin precedentes. La libertad de expresión es un pilar fundamental de las sociedades democráticas. Sin embargo, la desinformación en línea amenaza este principio al crear un entorno hostil para el debate público inclusivo y plural. La obligación principal de los agentes estatales reside en prevenir la interferencia y garantizar un entorno propicio para la discusión pública.

Agentes tanto nacionales como extranjeros pueden capitalizar la desinformación en línea para manipular políticas, debates sociales y comportamientos en varios ámbitos, incluyendo el cambio climático, migración, seguridad pública, salud y finanzas. En este sentido, en la comunicación ya se ponía de manifiesto cómo las plataformas en línea, especialmente las redes sociales y los motores de búsqueda, juegan un papel crucial en la difusión y amplificación de la desinformación. La comunicación constataba como hasta ese momento no se habían tomado medidas proporcionadas para mitigar este fenómeno. La Comisión Europea propuso ya en 2018 un enfoque a escala europea para garantizar una acción eficaz y coordinada que proteja a la UE, sus ciudadanos, sus políticas y sus instituciones contra la desinformación en línea.

Este documento sentó las bases para un Plan de Acción en Materia de Desinformación, cuyo objetivo es articular estrategias y medidas específicas para combatir la proliferación de noticias falsas y contenidos engañosos en la web.

Además, con la mirada puesta en fortalecer los valores democráticos, se estableció el Plan de Acción para la Democracia Europea. Este plan no solo enfatiza la necesidad de combatir la desinformación, sino que también desarrolla directrices claras sobre las responsabilidades y la rendición de cuentas que deben tener las plataformas en línea en este combate.

En 2018, se introdujo un hito en la lucha contra la desinformación: el Código de Buenas Prácticas en Materia de Desinformación. Esta iniciativa, pionera a nivel global, marcó la primera vez que la industria digital acordó, por iniciativa propia, un conjunto de normas de autorregulación para combatir la desinformación. El propósito principal de este código era cumplir con los objetivos trazados en la Comunicación de la Comisión presentada ese mismo año.

Un aliado esencial en esta batalla es el EDMO (Observatorio Europeo de Desinformación). Esta entidad independiente congrega a verificadores de hechos,

investigadores académicos especializados en desinformación en línea, plataformas de redes sociales y profesionales del periodismo y la alfabetización mediática. Su labor es crucial para analizar, entender y proponer soluciones a este fenómeno.

Por último, y reafirmando el compromiso de la UE con esta causa, en junio de 2022 se firmó un nuevo “Código de Buenas Prácticas en Materia de Desinformación” (Comisión Europea, 2022). Esta actualización busca involucrar a un espectro aún más amplio de actores en el compromiso voluntario de establecer y seguir prácticas que ayuden a contrarrestar la desinformación en todas sus formas. El Código de 2022 es una respuesta estructurada y multifacética en la Unión Europea para combatir este desafío.

El Código reforzado tiene como objetivo primordial desincentivar financieramente a los proveedores de desinformación. Para lograr esto, se establecen medidas enérgicas que previenen la colocación de publicidad junto a contenido desinformativo y la difusión de publicidad que contenga desinformación. Además, se promueve una cooperación eficaz entre los actores del sector publicitario, lo que permite una acción conjunta más robusta. Asimismo, reconoce la relevancia de la publicidad política en la configuración de la vida pública y compromete a los signatarios a implementar medidas de transparencia más estrictas. Estas medidas incluyen proporcionar un etiquetado eficiente de los anuncios políticos, revelar el patrocinador, el gasto publicitario y el período de visualización, además de establecer bibliotecas publicitarias eficientes y con capacidad de búsqueda.

Con el Código se refuerzan las medidas para reducir comportamientos manipulativos utilizados para difundir desinformación, como cuentas falsas, amplificación impulsada por bots, suplantación de identidad, y falsificaciones profundas maliciosas. Se promueve una cooperación ampliada entre los signatarios para combatir desafíos relacionados con estas técnicas, revisando periódicamente las tácticas, técnicas y procedimientos empleados por agentes malintencionados.

Es importante descartar como medida clave que se propone proteger a los usuarios de la desinformación a través de herramientas mejoradas para reconocer, entender y señalar la desinformación, así como acceder a fuentes autorizadas y participar en iniciativas de alfabetización mediática. Además, se establecerán prácticas de diseño seguras para limitar la difusión de la desinformación y garantizar una mayor transparencia en los sistemas de recomendación.

El Código prevé un mejor apoyo a la investigación sobre desinformación y amplía la cobertura del control de datos en todos los Estados miembros y lenguas de la UE. Se garantiza un uso más coherente de la verificación de datos en las plataformas, contribuciones financieras justas para los verificadores de datos, y un mejor acceso a la información que facilita su trabajo diario. Se establece un Centro de Transparen-

cia accesible a todos los ciudadanos para proporcionar una visión general fácil de la aplicación de las medidas del Código. Un Grupo Operativo mantendrá el Código actualizado y apto para su propósito mediante la revisión y adaptación de los compromisos ante la evolución tecnológica, social, de mercado y legislativa.

Se incluye un marco de seguimiento robusto con indicadores de nivel de servicio para medir la aplicación del Código en toda la UE y a nivel de los Estados miembros. Los signatarios presentarán informes de referencia sobre su aplicación del Código a la Comisión, y se comprometen a trabajar para establecer indicadores estructurales que permitan medir el impacto global del Código sobre la desinformación.

#### 4. ANÁLISIS DE LOS INFORMES DEL PARLAMENTO EUROPEO

De cara a las elecciones europeas de 2019, el Parlamento Europeo intensificó su papel contra la interferencia extranjera y la desinformación y decidió el 18 de junio de 2020 crear una Comisión Especial sobre Injerencias Extranjeras en todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación. Tras 50 audiencias con más de 130 expertos, el 9 de marzo de 2022 el pleno del Parlamento Europeo adoptó la Resolución de la Comisión Especial por 552 votos a favor, 81 votos en contra y 60 abstenciones. Y un día después, el 10 de marzo, el pleno aprobó el mandato de una nueva Comisión Especial (ING2) por abrumadora mayoría, con 614 votos a favor, 42 en contra y 34 abstenciones, que pasó a denominarse la nueva Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación, y sobre el Refuerzo de la Integridad, la Transparencia y la Rendición de Cuentas en el Parlamento Europeo tenía un mandato de 12 meses y tiene la responsabilidad de dar seguimiento al informe del INGE 1. Sobre la base del trabajo de INGE 2, el Pleno del Parlamento aprobó una resolución el 1 de junio de 2023, (Parlamento Europeo, 2023) en la que resalta una preocupación creciente sobre las injerencias extranjeras en los procesos democráticos dentro de la Unión Europea (UE). Esta resolución detalla distintos ámbitos de injerencia, subrayando la participación de actores externos, principalmente Rusia y China, en la desestabilización de la integridad democrática de la región. La discusión se extiende sobre varios temas críticos incluyendo la manipulación de plataformas en línea, protección de infraestructuras esenciales, intromisión en los procesos electorales y la ciber resiliencia. El PE pone en manifiesto la imperante necesidad de abordar la microsegmentación de la publicidad política, especialmente aquella basada en datos personales sensibles. Se expresa una notable insatisfacción hacia las empresas de redes sociales por no asumir plenamente su responsabilidad en la identificación y eliminación eficaz de la desinformación. Además, resalta una dependencia preocupante

de la UE hacia empresas extranjeras para preservar la integridad de las elecciones europeas. Para contrarrestar esto, se sugiere una mayor coordinación entre las plataformas para identificar y detener campañas de desinformación, así como incrementar la financiación y la integración de verificadores de datos externos acreditados en todas las lenguas de la UE. También se insta a las plataformas a priorizar la información basada en hechos provenientes de fuentes fiables y a facilitar el acceso, especialmente a los investigadores, para un mejor análisis y supervisión del contenido en línea. Asimismo, el Parlamento propone la inclusión de la infraestructura electoral digital y los sistemas educativos en la lista de infraestructura crítica. Se recomienda que la Comisión desarrolle legislación sobre la seguridad de la cadena de suministro de tecnologías de la información y la comunicación, y un marco regulatorio más sólido para armonizar las prácticas nacionales de control de la inversión extranjera directa. Además, sugiere la posibilidad de bloquear la inversión extranjera directa que sea perjudicial para los intereses de la UE. En una medida de precaución, se recomienda que la Comisión y el Consejo excluyan equipos y software de países de alto riesgo, extendiendo la prohibición de TikTok a todas las instituciones de la UE. Por otra parte, en relación con las injerencias durante los procesos electorales, el PE subraya la necesidad de fortalecer las herramientas disponibles para la Autoridad para los Partidos Políticos Europeos y las Fundaciones Políticas Europeas, con el objetivo de rastrear eficazmente las donaciones y garantizar una participación plena del Parlamento en este proceso. Se sugiere que la Comisión elabore un código de buenas prácticas dirigido a los representantes y autoridades públicas en las redes sociales. Además, se insta a los Estados miembros de la UE a implementar salvaguardias legales que prevengan la recepción de pagos de origen extranjero por parte de los partidos políticos europeos. Se propone la creación de redes de cooperación en materia electoral similares a la existente a nivel europeo, extendiendo la colaboración a los Parlamentos nacionales de la UE. También se enfatiza en la necesidad de que los gobiernos estatales y locales de la UE estén equipados con servicios y herramientas adecuadas para combatir las interferencias en los medios de información. Para contribuir a una mayor resiliencia de la ciudadanía, propone una estrategia coordinada de alfabetización mediática a nivel de la UE, compartiendo directrices con países candidatos. Se sugiere el establecimiento de un Observatorio de Influencias Extranjeras para analizar los impactos de las interferencias en la educación superior y la investigación. Además, se insta a fortalecer la capacitación y las acciones de conciencia situacional entre las instituciones, organismos y agencias de la UE y los estados miembros. Se aboga por una financiación suficiente y sostenible para apoyar a periodistas de investigación y organizaciones de la sociedad civil que se dedican a explorar estos temas. Tema aparte es el espacio que dedica a la financiación encubierta de actividades políticas, respecto a la cual destaca la necesidad de identificar normas comunes de la UE en lo que

respecta a campañas políticas y financiación de partidos políticos. Se expresa la expectativa de que las negociaciones en curso fortalezcan el mandato de la Autoridad para los Partidos Políticos Europeos y las Fundaciones Políticas Europeas, particularmente en lo que respecta a las transacciones financieras provenientes de países no pertenecientes a la UE. Se enfatiza la urgencia de adoptar medidas sobre transparencia y focalización de la publicidad política antes de las elecciones europeas de 2024, y se propone la prohibición de publicidad financiada por actores fuera de la UE y del EEE. Además, se invita a los Estados miembros a abordar el tema de las donaciones de terceros países a partidos nacionales. Respecto al impacto de la injerencia en los derechos de las minorías y otros grupos vulnerables, se enfatiza en la importancia de desarrollar programas a largo plazo que respalden a organizaciones de base locales y a las iniciativas ciudadanas en la resistencia al extremismo de derecha. Se insta a las instituciones, organismos y agencias de la UE, junto con las autoridades nacionales, a monitorear y desacreditar la desinformación rusa sobre la guerra en Ucrania y los refugiados ucranianos. También se subraya la necesidad de proporcionar información accesible de verificación de datos para combatir la desinformación, garantizando el acceso a la información en todos los formatos posibles para personas con discapacidad. Por último, se propone la creación de sistemas de alerta temprana para identificar y denunciar la desinformación de género, y se solicita una investigación sobre las fuentes de financiación de las campañas de desinformación de género.

## 5. LEY DE SERVICIOS DIGITALES

La Ley de Servicios Digitales (DSA, por sus siglas en inglés) representa una trascendental iniciativa europea destinada a renovar y actualizar el marco legal vigente en la Unión Europea, haciendo especial énfasis en la modernización de la Directiva de Comercio Electrónico del año 2000. Esta renovación legal se instaura como una respuesta a los desafíos emergentes y evolutivos asociados con el mundo digital y las plataformas en línea, proponiendo una arquitectura reguladora que resguarda tanto la seguridad de los usuarios como la integridad y transparencia de los espacios digitales. En el núcleo de la DSA se hallan varios objetivos cruciales que buscan, en primera instancia, forjar entornos en línea más seguros. Esto se logrará a través de la implementación de procesos específicos destinados a la moderación del contenido en línea, y mediante la armonización de las regulaciones de contenido a lo largo de toda la Unión Europea. Dicha armonización abarcará aspectos relacionados con el contenido ilegal, la publicidad transparente y la desinformación. En segundo lugar, se promueve una regulación uniforme de los proveedores de servicios digitales dentro del territorio de la UE. Este enfoque se integra en un conjunto

más amplio de proyectos regulatorios impulsados por la Comisión Europea, incluyendo también la Ley de Mercados Digitales (DMA). Finalmente, la DSA se centra en la protección de los derechos fundamentales de todos los usuarios de servicios digitales y en el establecimiento de un campo de juego nivelado que fomente la innovación, el crecimiento y la competitividad en el espacio digital de la UE. Profundizando en las modificaciones específicas introducidas por la DSA, se destacan varias medidas y obligaciones nuevas dirigidas hacia una mejor gestión y control del espacio digital. Entre estas, se incluyen las medidas para combatir la disponibilidad de bienes, servicios o contenidos ilícitos en línea, mediante la implementación de mecanismos que permitan a los usuarios reportar estos contenidos, y promoviendo la cooperación entre las plataformas y los denominados “alertadores fiables”. Además, se establecen nuevas obligaciones sobre la trazabilidad de las empresas usuarias en los mercados en línea, con el propósito de ayudar a localizar a los vendedores de bienes o servicios ilícitos. En lo que respecta a la protección de los usuarios, la DSA garantiza la posibilidad de impugnar las decisiones tomadas por los moderadores de contenidos de las plataformas, estableciendo así un marco de garantías efectivas. Se promulgan también medidas de transparencia de amplio alcance aplicables a las plataformas en línea, extendiéndose también a la divulgación sobre los algoritmos utilizados para recomendaciones. Para las plataformas de muy gran tamaño, que alcanzan a más del 10% de la población de la UE, se delinean obligaciones específicas destinadas a prevenir cualquier abuso de sus sistemas, mediante la adopción de medidas basadas en el riesgo y auditorías independientes de sus sistemas de gestión de riesgos. Los investigadores, por otro lado, tendrán acceso a los datos de las plataformas clave para examinar cómo funcionan, promoviendo así una comprensión más profunda y una mayor transparencia. Además, se fomentará la adopción de códigos de conducta y normas técnicas que ayudarán a las plataformas y a otros agentes a cumplir con las nuevas normas, mientras que otros códigos se implementarán para mejorar las medidas adoptadas en garantizar la accesibilidad de las plataformas.

## 6. ASAMBLEA PARLAMENTARIA DE LA OTAN

Pasamos ahora a analizar el tema desde el enfoque Parlamentario de la OTAN. Así, en el informe titulado “Bolstering the democratic resilience of the alliance against disinformation and propaganda” la ponente Linda Sánchez señaló como el escenario global contemporáneo se halla inmerso en una vorágine informativa, en la cual diversos actores, tanto internos como externos, participan activamente. Desde estados autoritarios hasta ciudadanos comunes, se ven involucrados en actividades

de información hostiles, con el objetivo de avanzar en sus intereses particulares. Esta dinámica representa una amenaza palpable para la seguridad y la resiliencia democrática de los aliados, al socavar los cimientos liberales sobre los cuales se erigen sus sociedades. La desinformación y la propaganda emergen como herramientas potentes en manos de aquellos que buscan perturbar el orden democrático. Al limitar el acceso a información verificada, estas prácticas incrementan la polarización social y erosionan la confianza en los procesos electorales, pilares fundamentales de las democracias. La situación se agrava con el creciente número de actores involucrados en la diseminación de desinformación y propaganda. Entre estos actores destacan estados autoritarios como Rusia, China e Irán, además de actores no estatales y ciudadanos individuales que, motivados por diversas razones, contribuyen a la difusión de narrativas dañinas. Estas actividades, deliberadas o no, explotan las vulnerabilidades tanto democráticas como tecnológicas presentes en las sociedades aliadas. Ante este panorama, el Comité Especial de la Asamblea parlamentaria de la OTAN propone un conjunto de medidas dirigidas a fortalecer la resiliencia democrática y tecnológica de las naciones aliadas. En primer lugar, se enfatiza la necesidad de consolidar la cohesión interna en torno a los valores y procesos democráticos que definen a estas sociedades. Este fortalecimiento de la cohesión interna se percibe como un escudo efectivo contra las amenazas emergentes en el espacio informativo. En segundo lugar, se subraya la importancia de desarrollar resiliencia tecnológica ante los embates de la desinformación y la propaganda. La resiliencia tecnológica se traduce en la capacidad de prevenir, detectar y responder ante las incursiones informativas hostiles. Adicionalmente, se propone fomentar la alfabetización mediática y digital entre los ciudadanos, así como brindar apoyo a los actores que operan en este campo crucial. La educación en medios y la competencia digital son vistas como pilares para la construcción de una sociedad informada y crítica. Por último, se promueve el incremento de la cooperación interparlamentaria como una estrategia viable para contrarrestar la desinformación y la propaganda. A través de una colaboración más estrecha entre los parlamentarios de las naciones aliadas, se busca crear un frente unido que permita abordar y mitigar los riesgos asociados a la desinformación y la propaganda en el ámbito internacional.

## 7. ANÁLISIS DE LOS INFORMES DEL CONSEJO DE EUROPA

La Resolución 2326 (2020) titulada “¿Democracia Hackeada? ¿Cómo Responder?”, emanada de la Asamblea Parlamentaria del Consejo de Europa, destaca una inquietud creciente respecto a las tendencias de interferencia electoral extranjera y manipulación digital, así como el comportamiento abusivo y la intensificación del

discurso de odio en internet y redes sociales. Esta resolución recuerda las preocupaciones previamente planteadas en resoluciones y recomendaciones anteriores sobre los desafíos legales asociados a la guerra híbrida y las obligaciones relativas a los derechos humanos. Se pone énfasis en el fenómeno emergente de la publicidad opaca o “dark advertising” en redes sociales en el marco de las campañas electorales basadas en datos. Se aboga por una regulación robusta que garantice la transparencia y la protección de datos, reconociendo el carácter transnacional del problema. Además, se enfatiza en la promoción de la educación mediática y las habilidades de alfabetización digital, así como en incentivar iniciativas de verificación de hechos y mejoras en la moderación de contenido. Se apoya, igualmente, a los investigadores dedicados a examinar la influencia de la desinformación en los procesos democráticos. En su análisis, la resolución subraya que la interferencia extranjera ya no se limita solo a los procesos democráticos, sino que se extiende a todos los aspectos del funcionamiento democrático, formando parte de estrategias de desestabilización o guerra híbrida. Las tácticas de interferencia adoptan diversas formas, incluyendo campañas de desinformación a gran escala, manipulación de plataformas de redes sociales, ciberataques, uso de programas de vigilancia ilegales y a gran escala, financiación encubierta de actividades políticas, captura y cooptación de élites, corrupción, y toma de control de infraestructura crítica. La propuesta de resolución presentada por D<sup>a</sup> María Valentina Martínez Ferro y otros miembros de la Asamblea, titulada “Interferencia Extranjera: una amenaza a la seguridad democrática en Europa”, refleja un compromiso profundo hacia la identificación y mitigación de las amenazas que implica la interferencia extranjera para la seguridad democrática en Europa. Resalta la creciente incidencia y la sofisticación de los intentos de interferencia extranjera, postulando un llamado urgente a fortalecer las estrategias de resiliencia y respuesta frente a estos desafíos.

## 8. CONCLUSIÓN

La problemática de la desinformación en línea ha captado la atención de diversas instituciones tanto a nivel europeo como transatlántico. El análisis de los documentos e informes emanados de la Comisión Europea, el Parlamento Europeo, la Asamblea Parlamentaria de la OTAN y la Asamblea del Consejo de Europa, nos brinda un panorama comparativo sobre cómo estas entidades perciben y enfrentan este desafío.

La Comisión Europea ve la desinformación en línea como un aspecto que requiere una estrategia integral. En este sentido, ha trazado acciones coordinadas y regulaciones para supervisar las plataformas digitales y redes sociales, buscando promover la transparencia y la responsabilidad. Además, enfatiza la importancia de la

cooperación entre diferentes sectores y la alfabetización mediática para contrarrestar la desinformación.

Por su parte, el Parlamento Europeo centra su atención en la resistencia democrática y en la protección de los procesos electorales ante posibles interferencias extranjeras y desinformación. Propone un marco regulatorio más riguroso en lo que respecta a la publicidad política y la financiación de partidos, además de impulsar la transparencia y la rendición de cuentas en las plataformas en línea.

La Asamblea Parlamentaria de la OTAN, por su parte, se enfoca en fortalecer la resiliencia democrática y tecnológica frente a la desinformación y la propaganda. Aboga por una mayor alfabetización mediática y digital, así como por una cooperación interparlamentaria internacional para tratar los desafíos que la desinformación plantea a nivel global.

La Asamblea del Consejo de Europa, ve la interferencia extranjera y la desinformación dentro de una estrategia de guerra híbrida. Sostiene la necesidad de una regulación robusta que garantice la transparencia y la protección de datos, y promueve la educación mediática junto con la verificación de hechos.

En lo que concierne a puntos de coincidencia, todas las instituciones resaltan la alfabetización mediática y digital como herramienta clave en la lucha contra la desinformación. También coinciden en la necesidad de regulaciones más sólidas para asegurar la transparencia y responsabilidad de las plataformas en línea, y en la cooperación tanto a nivel interinstitucional como internacional para enfrentar la desinformación y la interferencia extranjera.

Este análisis comparativo revela una convergencia en la identificación de la desinformación en línea como una amenaza significativa para la democracia y la estabilidad en Europa y la OTAN. Sin embargo, las variaciones en los enfoques y el grado de regulación propuesta reflejan las diferentes perspectivas de cada institución. La cooperación interinstitucional e internacional, la alfabetización mediática y la transparencia se destacan como temas recurrentes en las propuestas de todas las instituciones, brindando una visión holística de cómo estos cuerpos europeos y transatlánticos perciben y buscan abordar la desinformación y la interferencia extranjera en el ámbito digital.

En conclusión, el análisis comparativo revela una convergencia en la percepción de la desinformación en línea y la interferencia extranjera como amenazas significativas, con una llamada unánime hacia estrategias integradas y coordinadas para mitigar estos desafíos. La desinformación en línea no es solo una amenaza contemporánea, sino un campo de batalla en el cual la integridad democrática y la estabilidad están en juego, requiriendo una acción colectiva y medidas reguladoras sólidas para salvaguardar los valores y procesos democráticos en la era digital.

## 9. BIBLIOGRAFÍA UTILIZADA

- Comisión Europea. (2018). La Lucha Contra la Desinformación en Línea: Un Enfoque Europeo. (COM(2018) 236 final). Recuperado de [<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52018DC0236#:~:text=COM%282018%29%20236%20final,en%201%C3%ADnea%3A%20un%20enfoque%20europeo>]
- Comisión Europea. (2022). El Código de Buenas Prácticas en Materia de Desinformación. Recuperado de [<https://digital-strategy.ec.europa.eu/es/policies/code-practice-disinformation>]
- Sanchez, L. (2021). Bolstering the Democratic Resilience of the Alliance Against Disinformation and Propaganda. *NATO Parliamentary Assembly*. <https://www.nato-pa.int/document/013-cds-21-edemocratic-resilience-against-disinformation-and-propaganda-report-sanchez>
- Parlamento Europeo (2022a). Informe de la Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación (A9-0022/2022), 8 de febrero.
- Parlamento Europeo (2022b). Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación [2020/2268(INI)]. Recuperado de [https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064\\_ES.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_ES.pdf)
- Parlamento Europeo. (2023). Resolución del Parlamento Europeo, de 1 de junio de 2023, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación. Recuperado de [https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219\\_ES.html](https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219_ES.html)
- Parlamento Europeo y Consejo de la Unión Europea. (2022). Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un Mercado Único de Servicios Digitales y por el que se modifica la Directiva 2000/31/CE (Ley de Servicios Digitales) (Texto pertinente a efectos del EEE). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R20651>
- Rid, T., & Fontal, Y. (2021). *Desinformación y guerra política : historia de un siglo de falsificaciones y engaños* (Ser. Letras de crítica). Crítica.
- Servicio Europeo de Acción Exterior (2021). EEAS Special report update: Short assessment of narratives and disinformation around the COVID-19 pandemic (Update December 2020 - April 2021). <https://euvsdisinfo.eu/uploads/2021/04/EEAS-Special-Report-Covid-19-vaccine-related-disinformation-6.pdf>

Wardle, C., Derakhshan, H., & Council of Europe. (2017). Information disorder : toward an interdisciplinary framework for research and policymaking (September 27, 2017, Ser. Council of Europe report, dgi, 2017, 09). Council of Europe. <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>