

# La veracitat periodística com a garantia de seguretat a la Unió Europea

Gerard Gros Muñoz  
Universitat Autònoma de Barcelona  
[gerardgross93@gmail.com](mailto:gerardgross93@gmail.com)



Recepció: 12/07/2024  
Acceptació: 02/09/2024  
Publicació: 31/01/2025

**Cita recomanada:** GROS MUÑOZ, G. (2025). "La veracitat periodística com a garantia de seguretat a la Unió Europea". *Quaderns IEE: Revista de l'Institut d'Estudis Europeus*, 4(1), 60-86.  
DOI: <<https://doi.org/10.5565/rev/quadernsieve.88>>

## Resum

---

La seguretat és sempre un dels objectius principals que busca protegir qualsevol Estat o organització internacional, com la Unió Europea. Aquesta seguretat, tanmateix, pot veure's afectada per determinades pràctiques, com és el cas de la desinformació. És per això que en els darrers anys des de les institucions europees s'ha posat èmfasi a intentar abordar aquesta problemàtica a través de diferents mesures i l'aprovació de nova legislació que pot contribuir-hi, com la *Digital Services Act*. De la mateixa manera, en aquesta tasca també hi tenen importància altres actors, com els mitjans de comunicació i les xarxes socials, que han de vetllar perquè la informació que hi publiquin sigui verídica. Si la informació falsa es difon, pot tenir importants efectes en la seguretat i en les societats democràtiques. En aquest article s'analitzen alguns casos i mesures preses per part de la Unió Europea per tal de mitigar la desinformació i vetllar perquè la ciutadania rebi informació veraç, així com per poder controlar, en la mesura del possible, l'efecte que puguin tenir les pràctiques de desinformació en la seguretat del bloc comunitari.

**Paraules clau:** Desinformació; Seguretat; Veracitat informativa; Llibertat de premsa; Xarxes socials.

---

**Resumen.** *La veracidad periodística como garantía de seguridad en la Unión Europea*

---

La seguridad es siempre uno de los objetivos principales que busca proteger cualquier Estado u organización internacional, como la Unión Europea. Esta seguridad, sin embargo, puede verse afectada por determinadas prácticas, como en el caso de la desinformación. Por eso en los últimos años desde las instituciones europeas se ha puesto énfasis en intentar abordar esta problemática a través de diferentes medidas, así como con la aprobación de nueva legislación, como es la *Digital Services Act*, que pueda contribuir a mitigar estos riesgos. De la misma manera, en esta tarea también tienen importancia otros actores, como los medios de comunicación y las redes sociales, que deben velar por que la información que publiquen sea verídica. Si la información falsa se difunde, puede tener importantes efectos en la seguridad y en las sociedades democráticas. En este artículo se analizan algunos casos y medidas tomadas por parte de la Unión Europea para velar por que la ciudadanía reciba información veraz; así como para poder controlar, en la medida de lo posible, el efecto que las prácticas de desinformación puedan tener en la seguridad del bloque comunitario.

**Palabras clave:** Desinformación; Seguridad; Veracidad informativa; Libertad de prensa; Redes sociales.

---

**Abstract.** *Journalistic veracity as a guarantee of security in the European Union*

---

Security is always one of the main objectives that any State or international organization, such as the European Union, seeks to protect. However, security can be affected and undermined by certain practices, such as disinformation. This is why, in recent years, the European institutions have tried to address this problem through different measures and the passing of new legislation that can contribute to it, such as the Digital Services Act. In the same way, other actors have an important role in this task, such as the media and social networks, who must ensure that the information they publish is truthful. If false information is disseminated, it can have significant effects on security and democratic societies. This article analyses some cases and measures taken by the European Union to ensure that citizens receive accurate information, as well as to control, to the extent possible, the effect that disinformation practices may have on the security of the community bloc.

**Keywords:** Disinformation; Security; Informative veracity; Freedom of the press; Social media.

## Sumari

1. Introducció
  2. La llibertat de premsa i la veracitat periodística: dos elements bàsics en democràcia
  3. La seguretat: una qüestió nacional i també europea
  4. La lluita de la Unió Europea contra la desinformació com a garantia de seguretat
  5. Conclusions
  6. Referències
- 

## 1. INTRODUCCIÓ

La llibertat de premsa ha estat sempre un dels puntals de qualsevol democràcia liberal, incloent-hi les de la Unió Europea. Malgrat que no està present explícitament als tractats de la Unió Europea, sí que ho està en les constitucions dels Estats membres i es pot dir que és una llibertat que gaudeix d'un estat de salut relativament bo a escala del bloc comunitari, malgrat que a països com Hongria, Itàlia o Grècia ha empitjorat en els darrers anys. Tanmateix, que existeixi llibertat de premsa no implica que tot el que es publiqui sigui cert, i això pot afavorir a la desinformació interessada i pot tenir conseqüències molt greus per a qualsevol democràcia. En els darrers anys, de fet, els casos i campanyes de desinformació han anat en augment i s'han intensificat, i especialment per part de tercers actors, com poden ser la Xina o Rússia, que volen aconseguir influència i establir la seva posició en qüestions com, per exemple, la Guerra d'Ucraïna. En l'àmbit domèstic dels Estats membres, cada cop també és més fàcil creuar-se amb informacions de dubtosa veracitat. A més, la cada cop major diversitat de canals, especialment de xarxes socials com *TikTok* o *X* (abans *Twitter*), afavoreixen un abast major i molt més ràpid d'aquests missatges o continguts, la qual cosa és també molt perillosa. Per tant, és molt important investigar en aquest àmbit per poder tenir clar què suposa la desinformació i per tal de dissenyar campanyes i/o estratègies per a fer-li front.

Tot plegat pot influir a legitimar certes posicions i discursos, estigmatitzar certs col·lectius, polaritzar la societat i, en definitiva, pot afectar decisivament a l'hora de votar, que és l'expressió màxima de qualsevol democràcia consolidada. Aquestes ingerències també poden obrir escletxes a la seguretat i inestabilitat dels Estats i, en conseqüència, de la mateixa Unió Europea. Això es veu sobretot quan les societats ja estan molt polaritzades, com demostren casos d'agressions a diversos polítics a Alemanya o l'intent de magnicidi del primer ministre d'Eslovàquia, Robert Fico. És per això que s'ha d'actuar de manera contundent per reduir, atacar o mitigar aquesta desinformació i així assegurar un funcionament democràtic i correcte del sistema polític de la Unió Europea i dels seus Estats membres. De fet, això ja s'està fent a

diversos nivells dins la Unió Europea, i és això el que s'analitza en aquest article: com s'està actuant a la Unió Europea per tal de garantir la veracitat periodística i com això té relació amb afavorir una major seguretat dins del bloc comunitari i dels Estats que el formen.

Aquest article busca confirmar aquesta relació entre veracitat informativa i seguretat, és a dir, si com més es garanteix la veracitat informativa i més es combat la desinformació, més es garanteix la seguretat dins el mateix territori i sistema de la Unió Europea i els seus Estats membres. Per fer-ho, s'analitzen diverses mesures legals i iniciatives d'actuació que s'han pres a escala comunitària —especialment durant la darrera legislatura (2019-2024)— i també per part d'alguns Estats membres, com França o Espanya, per combatre la desinformació. En general, s'ha intentat vincular el màxim possible aquest article amb l'actualitat i amb casos i informacions recents.

## **2. LA LLIBERTAT DE PREMSA I LA VERACITAT PERIODÍSTICA: DOS ELEMENTS BÀSICS EN DEMOCRÀCIA**

La llibertat de premsa ha estat des de la consolidació de les democràcies liberals, a la segona meitat del segle XIX, un dret fonamental garantit per les constitucions i sistemes legals de molts països. A Europa, diversos països hi posen èmfasi en les seves lleis. És el cas de la República Francesa que, el 29 de juliol de 1881, va promulgar una llei sobre la llibertat de premsa, i que, malgrat anar patint canvis encara té vigència. També la Constitució de Bèlgica, que data del 1831, estableix la llibertat de premsa com una de les llibertats fonamentals, amb un text que resa així: “la premsa és lliure; la censura no podrà establir-se”.

Però, si ens fixem en definicions constitucionals respecte a la llibertat de premsa, una de les més destacables és la que fa la Constitució espanyola, que, a l'article 20.1, secció a, estableix la llibertat “a expressar i difondre lliurement els pensaments, les idees i les opinions mitjançant la paraula, l'escrit o qualsevol altre mitjà de reproducció”. A part d'això, estableix un altre punt remarcable en aquest mateix article 20.1, secció d: “Es reconeix i es protegeix el dret a comunicar o rebre lliurement informació veraç per qualsevol mitjà de difusió. La llei regularà el dret a la clàusula de consciència i al secret professional a l'exercici d'aquestes llibertats”. És a dir, d'alguna manera la Constitució espanyola relaciona la llibertat de premsa amb la difusió d'informació veraç. Aquesta darrera definició té en compte, doncs, que pot haver-hi informació no veraç o falsa.

El fenomen de la informació falsa i la desinformació s'ha intensificat en els darrers anys, tot i que, com destaquen García-Marín i Salvat Martinrey (2021), no constitueix un fenomen exclusiu del nostre temps. Relacionat amb aquesta desinformació, en els darrers anys s'ha vist també un creixement destacat de les anomenades *junk news*, que són informacions que, sense ser necessàriament falses, amaguen una agenda ideològica o política determinada (García-Marín i Salvat, 2021).

Diferents estudis estan d'acord en assenyalar que el fenomen general de la desinformació moderna es considera iniciat l'any 2016, coincidint amb la campanya presidencial als Estats Units, que va guanyar Donald Trump, i també amb el referèndum del Brexit al Regne Unit d'aquell mateix any (Mayoral, Parratt i Morata, 2019). Els mateixos autors, citant a Journell, Allcott i Gentzkow, asseguren que el fenomen té a veure amb les noves possibilitats de distribuir continguts de manera massiva a través d'internet (Mayoral, Parratt y Morata 2019). Noves eines, especialment les xarxes socials, s'han convertit en fonamentals per difondre desinformació de tota mena a través de textos, imatges, vídeos, mems o bots, com destaquen Alice Marwick i Rebecca Lewis (2017). Aquí també hi juga un paper més important el desenvolupament de la intel·ligència artificial, que ha ampliat les possibilitats de manipular textos, imatges, àudios o vídeos, amb contingut cada cop més realistes (Bontridder i Poulet; 2021).

A més, com assenyalen Colomina, Sánchez Margalef i Youngs (2021), les campanyes de desinformació són cada cop més sofisticades i "microorientades", mitjançant estratègies de màrqueting que utilitzen les dades de les persones per segmentar-les en grups reduïts, proporcionant així contingut a mida. En aquest context, hi juguen també un paper fonamental els algorismes que regeixen aquestes plataformes. La manera en què els algorismes governen directament el flux de notícies i d'informació, fent inferències a partir de grans conjunts de dades per determinar les preferències dels usuaris i així oferir missatges "microorientats", plantegen diversos problemes crítics d'interès públic (Hoffmann, Taylor i Bradshaw 2019).

Aquesta nou entorn digital comporta, doncs, que qualsevol persona o entitat (governos, empreses o grup d'interès) amb un compte de xarxes socials pot crear i difondre desinformació. En aquest context es pot fer una distinció general entre qui fabrica la informació i qui s'encarrega de difondre-la. D'una banda, hi ha els instigadors (directes o indirectes) que són els que creen els continguts; i, d'una altra, els agents (persones, funcionaris, grups, empreses o institucions), que són els encarregats de difondre les falsedats.

Per tant, es pot assegurar que la desinformació és una eina perillosa que pot interferir en drets tan bàsics com el dret a la llibertat de pensament i o el dret a la intimitat. En definitiva, com indiquen els mateixos autors, la desinformació disminueix la qualitat democràtica, ja que minva la confiança en les institucions democràtiques, pot arribar a distorsionar els processos electorals, fomenta la polarització i, inclús, l'incivisme (Colomina, Sánchez Margalef i Youngs, 2021).

A escala de la Unió Europea, es pot dir que la llibertat de premsa gaudeix d'un estat de salut bastant bo, si es compara amb la situació en l'àmbit global. Entre els deu primers classificats del rànquing sobre llibertat de premsa de 2024, elaborat per Reporters sense Fronteres, dels vuits primers països, set són de la Unió Europea (Dinamarca, Suècia, Països Baixos, Finlàndia, Estònia, Portugal, i Irlanda, per aquest ordre).<sup>1</sup> No obstant això, el mateix informe també destaca els retrocessos en aquesta matèria a països del bloc com Hongria, Eslovàquia, Grècia, Malta o Itàlia.

---

<sup>1</sup> Reporters Without Borders. *Index 2024*. <https://rsf.org/en/index>

Malgrat que cada país respecti la llibertat de premsa en la seva legislació, mai ha existit una normativa d'abast europeu per garantir la llibertat de premsa. Ni tan sols el mateix Tractat de la Unió Europea fa esment en cap moment a la llibertat de premsa, d'informació o a rebre informació verídica per part dels mitjans de comunicació. En canvi, pel que fa a la desinformació, les institucions europees i els Estats membres, han començat a crear algunes eines per assegurar la veracitat dels continguts que es publiquen o per desmentir aquells que siguin falsos o mitges veritats. Com es destaca des de la Comissió Europea, les campanyes de desinformació a gran escala són un repte important per a Europa i requereixen una resposta coordinada dels països de la UE, les institucions de la UE, les plataformes en línia, els mitjans de comunicació i els ciutadans de la UE (European Commission, 2022). Per tant, són molts els actors que han d'estar implicats per garantir la veracitat de les informacions i no caure en els paranys de la desinformació.

### 3. LA SEGURETAT: UNA QÜESTIÓ NACIONAL I TAMBÉ EUROPEA

La seguretat dels Estats ha estat sempre una de les grans preocupacions dels governants. Aquesta seguretat nacional inclou la defensa de qüestions més físiques, com les fronteres per exemple; i alhora de qüestions més abstractes, com la cultura o uns determinats valors. Com resumeix Caudle (2009), la seguretat nacional sembla centrar-se en la preservació d'allò que fa únic a un país, i això inclou els intangibles de la seva cultura, així com el que hi ha físicament dins de les seves fronteres. Amb aquest objectiu, la majoria d'Estats i governs han creat els seus propis organismes de seguretat nacional, com per exemple el *Departamento de Seguridad Nacional* a Espanya o la *Sûreté de l'État* a Bèlgica, per citar alguns exemples. De la mateixa manera, la Unió Europea també té el seu propi cos de seguretat, denominat *European Security Union*.

L'*European Security Union* i els departaments de seguretat nacional dels Estats membres han compartit les mateixes prioritats en els darrers anys, segons s'extreu dels informes que aquestes agències publiquen anualment. Entre aquestes, destaquen qüestions com la lluita contra les ingerències estrangeres, el terrorisme, els extremismes polítics i religiosos o el crim organitzat. Així mateix, i especialment des de l'esclat de la pandèmia de la Covid-19 i de la Guerra d'Ucraïna, la desinformació i les amenaces híbrides han agafat cada cop més protagonisme.

Dins del concepte amenaces híbrides, s'hi inclouen diverses pràctiques com la instrumentalització de l'alimentació, la migració irregular, l'energia o la manipulació i interferència d'informació estrangera. Per tant, una amenaça híbrida es pot definir com el fenomen resultant de la convergència i interconnexió de diferents elements que, en conjunt, constitueixen una amenaça més complexa i multidimensional (Pawlak; 2015). Dins d'aquest ampli concepte, se'n poden identificar d'altres més concrets, com el de guerra híbrida o el de conflicte híbrid. D'una banda, amb guerra híbrida es fa referència a la situació en què un país recorre a l'ús obert de la força armada contra un altre país o contra un actor no estatal, alhora que fa servir altres mitjans per exemple, econòmics,

polítics o diplomàtics. Quant al conflicte híbrid, s'entén com la situació en la qual les parts s'abstenen de l'ús obert de la força armada i actuen combinant la intimidació militar (sense arribar a un atac convencional) i l'explotació de vulnerabilitats econòmiques, polítiques, tecnològiques i diplomàtiques (Galán, 2018).

La preocupació per les amenaces híbrides queda molt clara, per exemple, a la Brúixola Estratègica per a la Seguretat i Defensa, aprovada pel Consell de la Unió Europea el març de l'any 2022. En aquest document, un dels objectius específics que s'hi estableixen és treballar amb socis per contrarestar les amenaces híbrides, la desinformació i els atacs informàtics.<sup>2</sup> En aquest àmbit és fonamental la cooperació de la Unió Europea amb els seus Estats membres i els seus socis occidentals a través de l'OTAN. Aquesta organització, en el seu informe estratègic de 2022, assegurava que s'invertirà en “la nostra capacitat de preparar-nos, dissuadir i defensar-nos de l'ús coercitiu de tàctiques polítiques, econòmiques, energètiques, d'informació i altres tàctiques híbrides per part dels Estats i actors no estatals”.<sup>3</sup> En aquest sentit, l'Aliança Atlàntica assenyala especialment dos països que suposen una gran amenaça per als seus interessos: la Federació Russa i la República Popular de la Xina.

Tanmateix, hi ha una gran diferència en el tracte que reben aquests dos països per part de l'OTAN i de les institucions europees. Amb la Federació Russa, la visió és plenament com a rival, i especialment des de l'esclat de la guerra d'Ucraïna, el febrer de 2022. En canvi, a la República Popular de la Xina se l'ha definit per part de la Comissió Europea al mateix temps com a rival sistèmic en l'àmbit polític, com a competidor econòmic, especialment en matèria tecnològica, i com a soci negociador en alguns aspectes d'interès comú entre les dues parts.<sup>4</sup>

De la mateixa manera, els serveis de seguretat nacional dels diversos Estats membres de la Unió Europea s'han anat expressant en una posició similar i han anat identificant diferents amenaces i prioritats que cal afrontar per garantir la seguretat dels respectius països. El *Secrétariat Général de la défense et de la sécurité nationale* francès, per exemple, ha posat molt èmfasi en les amenaces híbrides en l'àmbit cibernètic. Aquest organisme va informar de 831 intrusions al llarg de 2021 i destaca que les activitats delictives es dirigeixen principalment a entitats menys protegides, mentre que alhora, els delinqüents milloren constantment les seves capacitats d'atac, utilitzades amb finalitats nefastes, espionatge i desestabilització. Per aquesta raó, destaca que convé mantenir o intensificar tots els esforços per elevar el nivell de ciberseguretat de les entitats públiques, incloent-hi hospitals. En un sentit semblant s'ha expressat Bèlgica, país que al mateix temps té importància perquè acull la seu d'una gran part de les institucions de la Unió Europea. Aquest país, tanmateix, posa més el focus en l'espionatge, sobretot per part de Rússia, a institucions públiques però

---

<sup>2</sup> COUNCIL OF THE EUROPEAN UNION; “A Strategic Compass for Security and Defence- For a European Union that protects its citizens, values and interests and contributes to international peace and security”; 2022.

<sup>3</sup> OTAN; “NATO Strategic Concept 2022”

<sup>4</sup> EUROPEAN COMMISSION, “Comission reviews relations with China, proposes 10 actions”, 12 de març de 2019.

també a empreses privades. En aquest sentit, la *Sûreté de l'Etat* belga ha destacat l'expulsió de 21 espies, instal·lats a l'ambaixada russa a Brussel·les, i de 19 més que formaven part de la missió russa davant de la Unió Europea. De fet, els serveis de seguretat belgues asseguren que un dels grans riscos és de la ingerència russa en processos electorals, com ja va fer a les eleccions nord-americanes del 2016, al referèndum del Brexit, del mateix any, o a les eleccions presidencials franceses del 2017.

Finalment, a Espanya, el *Departamento de Seguridad Nacional* posa el focus en els mateixos aspectes, però també identifica la instrumentalització de la migració irregular com a amenaça a tenir en compte. El mateix organisme destaca que, recentment, especialment arran de la Guerra a la Franja de Gaza, Rússia està intentant projectar a la Unió Europea com una organització poc creïble i que dona suport a moviments imperialistes o "neocolonialistes" pel seu suport a Israel. A més, destaca que aquesta retòrica, per part del Kremlin, s'usa especialment dirigida cap a països de l'anomenat sud global (Àfrica i Amèrica Llatina) per guanyar influència en aquesta regió. En aquest sentit, també destaca el paper creixent de la Xina, que alinea el seu discurs amb Rússia pel que fa al rebuig cap als Estats Units i l'ordre internacional vigent, i ho fa especialment a través de les xarxes socials i els òrgans propagandístics del govern xinès, i dirigits sobretot cap al públic d'Amèrica Llatina.

Pel que fa als mitjans, destaca que cada cop la desinformació és més sofisticada (creada amb noves eines com la intel·ligència artificial) i difosa, de tal manera que cada cop és més difícil vincular-la amb la seva procedència i amb l'Estat que la crea. Per resoldre-ho, el *Departamento de Seguridad Nacional* posa èmfasi en la cooperació, que considera com a fonamental, ja que la complexitat del fenomen exigeix un coneixement de les seves causes profundes, íntimament lligades a la situació social, cultural, política i econòmica dels països als quals van dirigits els missatges.

Per tant, el que es planteja és un model d'estratègia de seguretat que s'ha de centrar en una gran varietat de rivals procedents de diferents àrees geogràfiques, que no reben el mateix tracte en funció de la seva rellevància en l'àmbit internacional, de les seves accions o sobre les mateixes prioritats de la Unió Europea i els seus Estats membres.

Alhora, aquestes amenaces són també molt diverses i cadascun d'aquests països rivals les utilitza de la manera més convenient. Per exemple, mentre que els països africans utilitzen sobretot la migració com a arma híbrida; grans potències, com la Xina o Rússia, fan servir altres mètodes més complexos, com les infiltracions cibernètiques o la interferència en processos polítics o electorals. En conseqüència, doncs, tant les institucions de la Unió Europea com les dels Estats membres han d'afrontar molts reptes plantejats per aquestes amenaces externes i, especialment, aquells que són veïns d'alguns d'aquests rivals, com és el cas d'Espanya amb el Marroc o dels tres països bàltics i Polònia amb Rússia i Bielorússia.

Aquí també cal remarcar que dins del marc de les institucions europees, s'han d'establir bé les principals prioritats i sobretot com afrontar-les, qüestió que pot ser a



vegades difícil d'equilibrar. És el que ha passat amb Rússia des de l'esclat del conflicte al Donbàs, el 2014. Mentre que països més propers geogràficament (Polònia, Estònia, Letònia i Lituània) volien una posició més ferma contra Rússia, en veure's més directament amenaçats; altres com Alemanya, liderada llavors per la cancellera Angela Merkel, no volien perjudicar les seves estretes relacions amb Rússia, país amb el que tenia, per exemple, una gran dependència energètica. Aquest objectiu, trobar posicions comunes en matèria de seguretat i mantenir relacions de manera comunitària amb tercers països, ha estat i és encara avui dia un dels grans reptes de la Unió Europea per poder afrontar aquests reptes de la manera més efectiva possible.

Per tant, es pot afirmar que la seguretat és un concepte molt ampli que inclou molts aspectes, situacions i actors implicats. De la mateixa manera, cal considerar que malgrat que existeix una Política Exterior i de Seguretat Comuna (que ahora inclou una Política Comuna de Seguretat i Defensa), com s'estipula a l'article 24 del Tractat de la Unió Europea, gran part de les competències en aquests àmbits encara són de cadascun dels Estats membres. Com a resultat, cada Estat membre actua en aquest àmbit segons els seus propis interessos, problemàtiques i mètodes, cosa que dificulta fer front comú davant certes amenaces o situacions, com passa per exemple amb la migració. Tanmateix, sembla que en els darrers anys s'està aconseguint millorar en aquest sentit, per exemple a través de l'adopció de quinze paquets de mesures sancionadores contra Rússia arran de la invasió d'Ucraïna<sup>5</sup> o a través de les tres qualificacions que ha rebut la Xina, sent ahora un país considerat com un rival sistèmic, competidor econòmic i soci negociador.

#### **4. LA LLUITA DE LA UNIÓ EUROPEA CONTRA LA DESINFORMACIÓ COM A GARANTIA DE SEGURETAT**

Tenint clars els dos conceptes bàsics sobre els quals es basa aquest article, la qüestió principal és fins a quin punt pot actuar la Unió Europea per fer polítiques de lluita contra la desinformació i d'aplicar-les dins el seu territori. En els darrers anys, la Unió, les seves institucions i els Estats membres han tractat d'actuar àmpliament en aquest àmbit, i especialment arran de moments com la pandèmia de la Covid-19 o l'agressió russa a Ucraïna, iniciada el febrer del 2022. Tots dos fets han estat un caldo de cultiu idoni per a la propagació de notícies falses, desinformació i teories de la conspiració, especialment, a través de plataformes virtuals i xarxes socials, com *X*, *Facebook* o *TikTok*.

---

<sup>5</sup> El nombre de paquets de sancions corresponen al moment de la publicació d'aquest article. En aquest web es troba la informació actualitzada: <https://www.consilium.europa.eu/es/policies/sanctions-against-russia/>

#### 4.1. La *Digital Services Act*

La gran referència legislativa europea és la *Digital Services Act* (DSA, en endavant), aprovada pel Parlament i el Consell de la Unió Europea el 19 d'octubre de 2022.<sup>6</sup> Aquest text té diversos punts importants que cal destacar pel que fa a la mitigació de riscos relacionats amb la desinformació. El reglament convida a les plataformes d'internet i a les xarxes socials a "avaluar com s'utilitzen els seus serveis per difondre o ampliar contingut enganyós, inclosa la desinformació, i reflectir-ho en les avaluacions de risc". També obliga a les grans plataformes i a les grans eines de cerca a diverses mesures, com l'adaptació dels seus termes i condicions (i garantir la seva aplicació), l'adaptació dels algorismes i els sistemes de recomanació de continguts, de publicitat i dels processos de moderació de contingut, entre d'altres. Al mateix temps, els obliga a prendre mesures en relació amb altres assumptes, com la protecció dels menors. Un altre punt important fa referència a l'ús de la intel·ligència artificial (IA, en endavant) i a la publicació d'imatges, àudios o vídeos modificats o generats per IA que mostrin persones, llocs, objectes o esdeveniments que semblin reals. En aquest sentit, obliga les plataformes a indicar explícitament que són falses o generades amb aquests mètodes, posant en marxa també opcions a les seves plataformes que permetin als usuaris indicar-ho correctament i de manera clara.

A l'hora de lluitar contra la desinformació, la Comissió Europea destaca de manera explícita que sempre s'han de respectar els drets fonamentals en qualsevol acció presa amb aquest objectiu, tal com s'infereix del codi reforçat de pràctiques contra la desinformació publicat per aquesta institució, l'any 2022. Entre els signataris del codi trobem plataformes i empreses com Google, Meta, TikTok, YouTube o X (llavors, Twitter). Tanmateix, aquest codi només suposa un compromís entre aquestes parts, i no és de caràcter obligatori. Per tant, una part important de l'èxit en la lluita contra la desinformació passa per si les empreses i plataformes signants compleixen amb els compromisos que han signat, malgrat no ser obligatoris, i per com ho fan. Al mateix temps, s'hi ha d'afegir la manera d'actuar conforme reglaments com la Llei de Serveis Digitals

Entre les mesures que han d'adoptar aquestes plataformes "molt grans" s'hi inclouen diverses accions, que es poden dividir en quatre blocs. En primer lloc, hi ha aquelles que estan centrades a afavorir un major empoderament dels usuaris, facilitant que aquests puguin denunciar continguts fàcilment o prohibint la presència de publicitat basada en dades delicades de l'usuari (orientació sexual, opinions polítiques...). El segon dels pilars d'actuació se centra en la protecció dels menors d'edat, segons les quals, les plataformes hauran d'actuar per assegurar-ne la privacitat i seguretat, alhora que tindran prohibida l'exhibició de publicitat dirigida a infants i adolescents. El tercer punt d'acció se centra en el control dels continguts, amb l'objectiu de reduir la desinformació. En aquest àmbit, hauran de prendre mesures (el text no

---

<sup>6</sup> Regulation (EU) 2022/2065 of the European Parliament and the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

especifica quines exactament) per afrontar els riscos lligats a la difusió de contingut il·legal o que pugui afectar negativament a les llibertats d'informació i d'expressió. Alhora, les plataformes hauran d'analitzar els seus propis riscos i fer el possible per mitigar-los. Finalment, el quart bloc de mesures va enfocat a aconseguir una major transparència a través d'auditories independents que comprovin el compliment de la DSA, posant la informació i les dades disponibles per al públic i publicar informes de transparència sobre la gestió de riscos i els controls de continguts. Amb tot plegat, doncs, es vol garantir una major transparència i responsabilitat per combatre la desinformació en aquests espais cibernètics.

#### **4.2. L'acció dels Estats membres contra la desinformació**

Addicionalment, alguns Estats membres han anat introduint mesures a escala nacional. Un exemple és França que, amb la Llei 2018-1202, del 22 de desembre de 2018, sobre la lluita contra la manipulació de la informació, se centra bàsicament a lluitar contra la difusió i incidència d'informacions falses en períodes electorals. En aquest text legislatiu es preveuen, entre d'altres, sancions econòmiques o de presó, si no es compleixen els estàndards de transparència requerits per la llei electoral<sup>7</sup> o la possibilitat que, durant els tres mesos anteriors a algun procés electoral o referèndum, els jutges puguin interposar accions judicials ràpides (a demanda de la Fiscalia, d'un candidat o partit, o persona interessada) per frenar la propagació d'una publicació sempre que es demostrï que és objectivament falsa, que es difon massivament i de manera artificial i que pot afectar a la pau social o a la veracitat de les eleccions en qüestió. Aquestes accions, però, només es poden dur a terme des de jutjats de gran instància i d'un tribunal d'apel·lació establerts per decret. De la mateixa manera, el text estableix obligacions per als operadors de plataformes en línia i xarxes socials. En aquest sentit, la llei obliga aquests operadors a establir un dispositiu de senyalament visible i de fàcil accés que permeti als usuaris denunciar informacions falses o errònies, una major transparència dels algorismes usats per recomanar o classificar continguts informatius, a la promoció de continguts fiables o a prendre mesures contra comptes que propaguin informació falsa, entre altres mesures.

A Espanya, el principal marc normatiu per a la lluita contra la desinformació és la Llei 36/2015 de Seguretat Nacional, que a l'article 11 estableix que les administracions públiques amb competències en matèria de seguretat nacional han d'establir mecanismes de coordinació i intercanviar informació per detectar i neutralitzar riscos i amenaces, inclosa la desinformació (Alastuey, 2024).

Igualment, cal destacar l'Ordre PCM/1030/2020 que va aprovar el Procediment d'Actuació contra la Desinformació, que busca establir mecanismes per estudiar i afrontar la desinformació i la seva influència en els àmbits global i nacional. L'execució

---

<sup>7</sup> JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE. "Loi 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information"; Article L.163-1.

d'aquest Pla es divideix en quatre fases. Primerament, es detecta la campanya desinformativa i s'analitza. A continuació, s'avalua l'impacte i es proposen mesures a través d'un mecanisme de coordinació interministerial, liderat per la *Comisión Permanente contra la Desinformación*. Seguidament, el Comitè de Situació s'encarregarà de la gestió estratègica i política de les mesures aprovades. Finalment, el *Consejo de Seguridad Nacional* durà a terme la direcció política i l'adopció de mesures pertinents d'alt nivell. A part d'aquests organismes, també participen altres òrgans, com les forces i cossos de seguretat, el *Centro Nacional de Inteligencia*, universitats, mitjans de comunicació i les plataformes digitals. Fruit d'aquesta col·laboració, un dels majors èxits ha estat la creació d'*Iberifier*, un observatori que agrupa entitats espanyoles i portugueses (mitjans de comunicació, universitats i plataformes de verificació) per fer front a la desinformació conjuntament. Durant el tercer trimestre de 2023, els verificadors que formen part d'aquest observatori van realitzar una mitjana de 245 verificacions.

Cal també destacar l'existència de lleis de transparència, que busquen, com s'explica al títol preliminar de la llei de transparència espanyola, "regular i garantir el dret d'accés a la informació relativa a l'activitat pública i establir les obligacions de bon govern que han de complir els responsables públics".<sup>8</sup> Aquests actors hauran de publicar periòdicament tota la informació necessària relacionada amb la seva activitat, per tal de garantir-ne la transparència i la possibilitat de control. Per tant, qualsevol ciutadà té dret a accedir o sol·licitar informació pública.

Tanmateix, hi ha límits a aquest dret d'accés, que inclouen, entre d'altres, la defensa i la seguretat nacional. Aquest últim pot ser un concepte molt ampli i, fins i tot, ambigu, que depèn de la interpretació de la institució en qüestió i, en conseqüència, pot suposar una limitació important al dret a l'accés a la informació i, de retruc, a la llibertat de premsa per investigar o publicar determinades informacions. En un sentit similar s'expressen la llei de transparència autonòmica de Catalunya<sup>9</sup> i les d'altres països europeus, que tampoc són gaire més clares en aquest aspecte. Així, doncs, les administracions públiques poden limitar de manera arbitrària l'accés a determinada informació, si consideren que s'adscriu a algun dels límits establerts.

De la mateixa manera, els Estats encara tenen marge per prendre més mesures respecte a la lluita contra la desinformació a escala estatal i són moltes les propostes que estan apareixent al respecte. El *Departamento de Seguridad Nacional* espanyol ha consultat experts i membres de la societat civil per posar sobre la taula possibles solucions o actuacions. A partir d'això conclou, per exemple, que seria idoni que existissin "òrgans, institucions i funcions definides normativament en l'àmbit governamental per identificar, detectar i monotonitzar la desinformació, acompanyat d'un reforç de la ciberseguretat i d'una major cooperació entre organismes, amb la

---

<sup>8</sup> Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

<sup>9</sup> Llei 19/2014 del 29 de desembre, de transparència, accés a la informació pública i bon govern, Art 21, pàg 34-35.

societat civil, amb el sector privat i l'àmbit acadèmic".<sup>10</sup> També afirma que hi ha marge per millorar la regulació i reduir els riscos legals a l'hora d'atacar la desinformació. També remarca que si s'ha de restringir alguna acció, contingut o pràctica considerada com a desinformació i que afecti la seguretat, les accions hauran de ser definides pels tribunals i no per l'administració, ja que posaria en risc la seguretat jurídica dels afectats.

El mateix grup de treball que ha participat en l'elaboració d'aquest informe del *Departamento de Seguridad Nacional* estima que també és fonamental garantir la transparència, especialment durant períodes electorals, però sempre respectant la llibertat d'expressió i el rol de la propaganda política. Per al grup, les eleccions han de convertir-se en una prioritat de seguretat nacional i les infraestructures electorals en una infraestructura crítica, dotant-les d'especial protecció per assegurar-ne el seu correcte funcionament. I això inclou, entre d'altres, mesures per a l'acció intensa contra la desinformació durant aquests períodes. En tot cas, això encara ha d'estar més ben regulat i alhora haurà de permetre que organismes com la *Junta Electoral Central* disposin dels recursos i capacitats adequades per poder actuar en aquest aspecte durant els períodes electorals. Per tant, encara hi ha molta feina per fer en aquests aspectes.

### 4.3. La desinformació russa i xinesa

Més enllà d'això, altres Estats membres no han aprovat projectes legislatius en matèria de desinformació tan ambiciosos. Tot plegat, és el que ha propiciat que la Comissió Europea decideixi actuar a escala comunitària per tal de crear un marc comú d'actuació contra aquesta problemàtica que cada cop es considera més important, com mostra l'aprovació de la *Digital Services Act*. A més, les institucions actuen també en funció de les circumstàncies o esdeveniments que poden afavorir la propagació d'informació falsa, com és el cas de la guerra entre Rússia i Ucraïna. Pel que fa a aquest conflicte, la Comissió Europea va publicar recentment un document on detalla l'aplicació del marc de gestió de riscos per a les campanyes de desinformació russes. En aquest sentit, la Comissió destaca el paper de les xarxes socials, i especialment de *Twitter* (actualment *X*) en la difusió de propaganda i desinformació per part del Kremlin. De fet, des d'aquesta institució es calcula que durant el primer any de guerra, aquestes campanyes arribaven a una audiència agregada de 165 milions de persones, que alhora suposa una xifra astronòmica de 16 bilions de visualitzacions a través de diferents actors, inclosos canals de televisió com *Russia Today*, comptes oficials del govern rus a les xarxes socials o d'*influencers* partidaris de la guerra que reproduïen les tesis del Kremlin. Alhora, destaca que cada cop hi ha més presència de comptes en aquestes plataformes

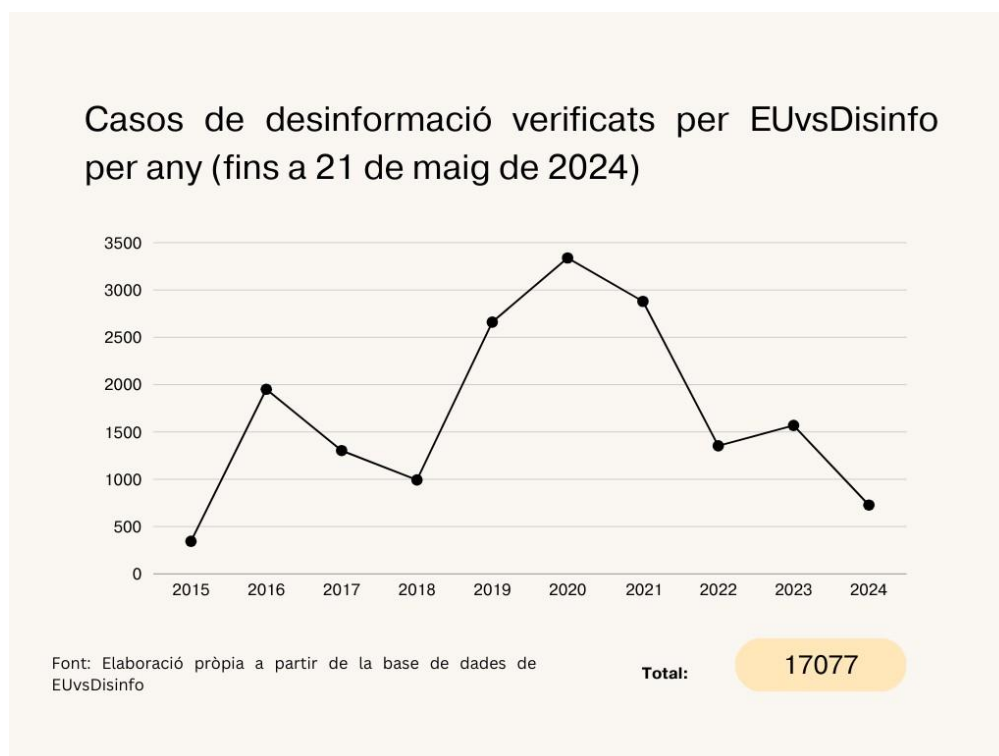
---

<sup>10</sup> DEPARTAMENTO DE SEGURIDAD NACIONAL. "Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil", pàg 72, 27 de setembre de 2022.

alineades amb Moscou i que encara s'han de fer molts esforços per poder mitigar els efectes de la desinformació per part de Rússia.

De fet, la desinformació per part de Rússia està present dins la Unió Europea des de molt abans de la guerra contra Ucraïna. Un dels organismes encarregat de fer-ho és el portal *EUvsDiSiNFO*, format per experts en el món comunicatiu i de les ciències socials amb coneixement de Rússia, que depèn de l'Alta Representació de la Unió per Afers Exteriors i Política de Seguretat. El grup, format el 2015, ha identificat i desmentit més de 17.000 casos de desinformació en diversos àmbits o temàtiques, tots disponibles a la seva base de dades. El grup destaca que el principal tema de desinformació és Ucraïna i que no és nou, sinó que va començar en 2014, amb l'inici de la crisi del Donbàs, per tal de "minar i desestabilitzar Ucraïna, semblant dubtes i confusió tant sobre el terreny com a ulls de la comunitat internacional". Com destaca aquest grup de treball, a més, des de la guerra a gran escala iniciada el 2022, la desinformació russa s'està intensificant i està arribant a públics de tot arreu i tractant altres temes com la seguretat alimentària o energètica, sempre amb l'objectiu de debilitar a Ucraïna. Per tant, la desinformació russa evoluciona i ho fa molt ràpidament.

L'evolució del nombre de continguts verificats per *EUvsDisinfo* ha passat per diferents fases al llarg dels anys, tal com es pot veure en el següent gràfic.



Les verificacions totals per any no han seguit una tendència estable. Entre el 2015 i el 2016 va haver-hi una pujada considerable, passant de 344 verificacions a 1.951. Després d'una baixada fins al 2018, a partir de llavors va començar un creixement molt exponencial fins a l'any 2020, quan, coincidint amb el sorgiment de la crisi de la Covid-19 i sent l'any més fort de la pandèmia, es va arribar a un rècord de

verificacions, amb un total de 3.339. Després d'una caiguda considerable els dos anys següents, amb la Guerra d'Ucraïna va haver-hi un petit repunt, especialment quan la guerra estava més equilibrada. Actualment, amb una millor situació al front bèl·lic per a Rússia, els casos verificats han tornat a baixar. Per tant, es pot veure que en els moments en què hi ha una situació més delicada les campanyes de desinformació s'intensifiquen i, per consegüent, es verifiquen més informacions falses.

Per tal de frenar això, *EUvsDiSiNFO* tracta d'oferir campanyes i eines de sensibilització, especialment a través de les xarxes socials. A X, per exemple, ja té més de 72.000 seguidors, i a *Facebook*, 70.000. A més, el contingut d'aquest òrgan es fa en diferents idiomes i, especialment, en aquells de països veïns o propers a Rússia, com són el romanès, l'armeni, l'ucraïnès o el georgià, ja que el públic d'aquests països pot ser el més vulnerable o procliu a caure en aquesta desinformació orquestrada pel Kremlin. Tanmateix, el mateix organisme admet que encara cal fer molta feina per contrarestar de manera eficaç l'ús de noves eines per difondre la desinformació, com ara els bots, la IA o, fins i tot, l'ús d'*influencers*.

Més enllà de Rússia, un altre actor molt actiu pel que fa a la desinformació dins de la Unió Europea és la República Popular de la Xina. Com es destaca a la Comunicació Conjunta sobre la lluita contra la desinformació al voltant de la Covid-19,<sup>11</sup> tant aquest país com Rússia han volgut minar el debat democràtic i augmentar la polarització arreu amb les seves campanyes de desinformació. En el cas de la Xina, les seves campanyes de desinformació solen anar dirigides bàsicament a "distreure", és a dir, a desviar l'atenció cap a un altre actor o narrativa, o a culpabilitzar a algun altre. Això la diferencia de Rússia, ja que la desinformació d'aquest país està més centrada en canviar el marc de les narratives.<sup>12</sup> Tenint en compte el gran volum de desinformació que genera la Xina, i que segurament anirà en augment en els pròxims anys, la Unió Europea ha desenvolupat també un grup de treball centrat en aquest país, que entre d'altres també inclou experts en desinformació.

Igualment, també s'han anat creant grups de treball centrats en altres zones geogràfiques, com el Nord d'Àfrica, l'Orient Mitjà o els Balcans Occidentals. Tot plegat s'orienta en les conclusions del Consell Europeu de juliol de 2022, que recorden "la necessitat de crear un conjunt d'instruments de la UE contra les amenaces híbrides que reuneixi diferents eines per detectar una àmplia gamma d'amenaces i campanyes híbrides i respondre-hi, i, en aquest context, desenvoluparà un conjunt d'instruments específics per fer front a la manipulació desinformació i la ingerència per part d'agents estrangers".<sup>13</sup> En definitiva, "reforçarà la [nostra] capacitat de detectar, analitzar i

---

<sup>11</sup> EUROPEAN COMMISSION. "Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling COVID-19 disinformation - Getting the facts right", pàg 4 10 de juny de 2020

<sup>12</sup> EUROPEAN EXTERNAL ACTION SERVICE. "1st EEAS Report on Foreign Information Manipulation and Interference Threats", pàg 5, febrer de 2023.

<sup>13</sup> COUNCIL OF THE EUROPEAN UNION. "Council conclusions on Foreign Information Manipulation and Interference (FIMI)"; 18 de juliol de 2022.

respondre a les amenaces, en particular imposant sancions als que duguin a terme aquestes activitats”.

#### 4.4. Afectacions de la desinformació al Parlament Europeu

Un altre esdeveniment sobre el qual es van detectar intents de desinformació i interferència per part d'alguns actors va ser la celebració dels comicis al Parlament Europeu, que es van realitzar entre el 6 i el 9 de juny del 2024. De fet, els eurodiputats van expressar la seva preocupació al respecte i van demanar prendre mesures per assegurar la integritat dels comicis i contrarestar les possibles campanyes de desinformació d'actors com la Xina o Rússia. En aquest sentit, els nous mecanismes legals derivats de la *DSA* o la *Artificial Intelligence Act* (AI Act, en endavant), aprovada el 13 de juny de 2024, seran essencials per frenar el risc d'ingerència i distorsió del procés democràtic per a futures eleccions. Per tant, la Unió Europea, dins les seves competències i funcions, està contribuint a combatre la desinformació.

Això no obstant, recentment, els serveis d'intel·ligència belgues i txecs han obert una investigació sobre possibles interferències russes en aquestes eleccions al Parlament Europeu a través d'una xarxa que busca minar el suport cap a Ucraïna. La xarxa en qüestió estaria oferint suborns a eurodiputats per promoure posicions prorusses.<sup>14</sup><sup>15</sup> Arran d'aquest cas, el Consell Europeu va subratllar, de nou, que els Estats membres i la Unió han de ser determinants per controlar qualsevol amenaça desinformativa (també la feta amb IA), de manipulació informativa des de tercers països i d'interferència en els processos electorals, i convidava a la cooperació entre les institucions europees i els Estats membres en aquest àmbit.<sup>16</sup>

Per a aquesta institució, també és destacable la ingerència de tercers països a través de la corrupció, que també és una forma d'amenaça híbrida. En aquest sentit, es pot destacar especialment el cas del *Qatargate*, destapat a finals de 2022, i que va afectar diversos eurodiputats de diverses nacionalitats, incloent-hi la ja ex-vicepresidenta del Parlament Europeu, Eva Kaili. En aquest cas, diversos eurodiputats van rebre diners de països com Qatar, Mauritània o el Marroc per defensar posicions favorables a aquests països a l'Eurocambra, com han anat revelant mitjans com l'alemany *Der Spiegel*<sup>17</sup> o el belga *Le Soir*.<sup>18</sup> Així mateix, sense sortir de Bèlgica, la premsa també ha revelat que un ex-senador i exdiputat al Parlament de Flandes pel partit d'extrema dreta independentista flamenc Vlaams Belang, Frank Creyelman,

---

<sup>14</sup> ASSOCIATED PRESS; “Belgium launches probe into suspected Russian interfering in upcoming EU elections”; 12 d'abril de 2024

<sup>15</sup> LA LIBRE BELGIQUE; “Alexander De Croo parle de l'ingérence russe sur les élections européennes”; 12 d'abril de 2024

<sup>16</sup> EUROPEAN COUNCIL. “Special European Council, 17-18 April 2024”.

<sup>17</sup> DER SPIEGEL; “Corruption scandal badly shakes European Parliament Credibility”; 16 de desembre de 2022.

<sup>18</sup> LE SOIR; “Messages WhatsApp, rendez-vous discrets et coups tordus: le lobbying pro-Qatar forcené d'Eva Kaili”; 8 de desembre de 2023.



havia estat tres anys actuant com a espia i enllaç pel règim xinès.<sup>19</sup> Tot això ho han pogut fer gràcies al fet que a ambdós països hi ha una llibertat de premsa sòlida, malgrat que es va erosionant al conjunt de la Unió.

En aquest sentit, cal destacar el treball que estan fent les institucions europees per intentar reforçar també la llibertat de premsa, per exemple a través de la coneguda com a *Media Freedom Act*. El Reglament, de l'11 d'abril de 2024, de 11 de abril de 2024, preveu mesures com la prohibició d'utilitzar *softwares* d'espionatge (per exemple, *Pegasus*) contra periodistes, la prohibició de les autoritats de pressionar els periodistes i editors per revelar les seves fonts o l'obligació als mitjans de deixar clar qui n'és el propietari.<sup>20</sup> Així mateix, el text preveu que les grans plataformes digitals distingeixin clarament el contingut dels mitjans independents i dels que no ho són, i preveu límits i condicions, en cas que es vulgui eliminar una publicació d'algun mitjà de comunicació en aquestes plataformes. Tanmateix, l'aprovació recent d'aquest text encara no està diluint escàndols relacionats amb la desinformació que afecten aquesta institució, com el *Russiagate*, pel qual, a finals de maig de 2024, la policia va fer registres al domicili i oficines d'un assistent d'un eurodiputat neerlandès acusat de promoure propaganda russa a través d'un "pseudomitjà" digital anomenat *The Voice of Europe*,<sup>21</sup> que es defineix al seu compte d'X com a "xarxa de notícies sense censura d'Europa i el món".

#### 4.5. "Pseudomitjans" i desinformació a les xarxes socials

Els "pseudomitjans" son cada cop més freqüents a la Unió Europea. Són pàgines web que es camuflen com a mitjans de comunicació o diaris digitals, però que realment s'utilitzen per difondre desinformació, propaganda o informació que, tot i ser potser certa, està creada clarament per aconseguir uns objectius o normalitzar una posició.

Si ens fixem en el cas anteriorment esmentat, *The Voice of Europe*, a la seva pàgina web s'hi poden veure moltes notícies relacionades amb la Guerra d'Ucraïna, però pràcticament totes sobre accions o impactes negatius per a Ucraïna, amb titulars de l'estil: "Irlanda retallarà les pensions i beneficis de discapacitat per als refugiats ucraïnesos"; "El president búlgar: La victòria d'Ucraïna sobre Rússia és impossible"; o "Noruega oferirà a centenars de refugiats ucraïnesos que abandonin el país". Totes aquestes informacions tenen la voluntat clara de mostrar que la Unió Europea o els seus aliats ja no tenen interès a ajudar a Ucraïna, amb un clar propòsit desestabilitzador. Per a casos com aquests, la *Media Freedom Act* ha de ser molt útil per identificar qui hi ha darrere d'aquests "pseudomitjans" i com es financen, i d'aquesta

---

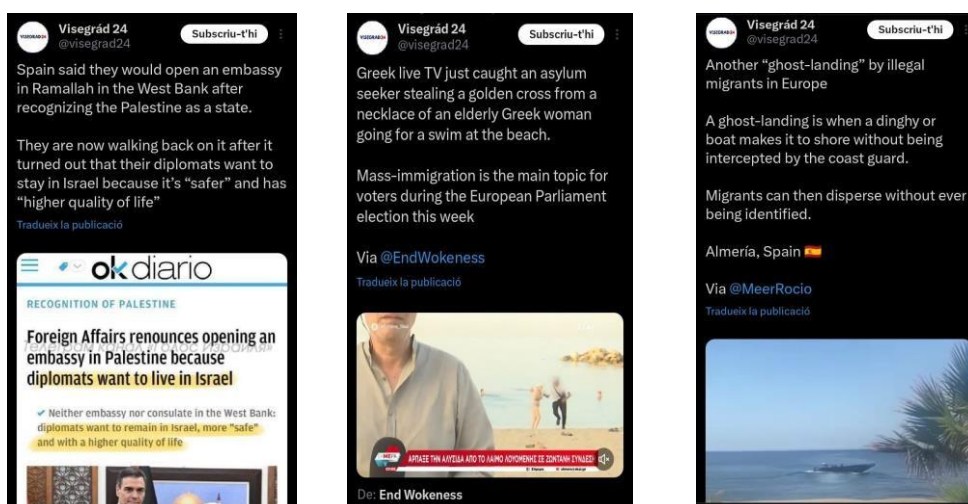
<sup>19</sup> FINANCIAL TIMES. "Chinese spies recruited European politician in operation to divide west", 15 de desembre de 2023.

<sup>20</sup> Reglamento (UE) 2024/1083 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se establece un marco común para los servicios de medios de comunicación en el mercado interior y se modifica la Directiva 2010/13/UE

<sup>21</sup> POLITICO. "Police raid EU Parliament offices in 'Russiagate' probe". 29 de maig de 2024.

manera tenir clar qui pot estar interferint dins la Unió i, en conseqüència, afectant la seguretat europea.

Això també succeeix a les xarxes socials, amb comptes i *influencers* que també s'encarreguen de difondre desinformació o informació molt interessada per desacreditar algunes posicions i polaritzar la societat. És el cas del compte anomenat *Visegrad24*, que compta amb un milió de seguidors a *X*, més de 33.000 a *Instagram* i més de 72.000 subscriptors a *YouTube*. El compte, fundat el 2020 pel polonès Stefan Tompson, podria haver tingut una relació propera amb l'anterior govern polonès, liderat pel partit ultraconservador Llei i Justícia (*Prawo i Sprawiedliwość*, PiS), tal com explica la web d'investigació periodística polonesa *OKO.press* (Mierzynska,2022). *Visegrad24*, per exemple, ha intentat desacreditar les protestes o mostres de suport a Palestina, que han tingut lloc arreu de la UE en el marc de la guerra de Gaza, acusant-les de violentes i antisemites i mostrant constantment imatges de manifestacions massives israelianes, com les del Dia de la Bandera, del 5 de juny de 2024, que tot i no mostrar-ho, sí que va acabar violentament. En aquest sentit, també s'ha mostrat clarament en contra del suport d'alguns governs de la UE, com l'espanyol, a Palestina. Més enllà d'això també se centra molt a criticar i desacreditar els immigrants que arriben a Europa i a l'Islam en general, intentant condicionar, fins i tot, el vot a les eleccions al Parlament Europeu de 2024. A més, sovint es fa ressò de notícies de comptes de xarxes socials i mitjans de dubtosa veracitat, com *OKDiario*; o, fins i tot, directament de diputats d'extrema dreta, com Rocío de Meer, diputada de Vox al Congrés dels Diputats per la circumscripció d'Almeria, com es pot veure a les captures de pantalla que es mostra seguidament:



Per tant, la desinformació no ve només d'actors externs a la UE, sinó també a través d'actors interns, com és aquest cas. I no ho fa només amb "pseudomitjans", ja que en l'era de les xarxes socials, també es fa amb *influencers*. En el cas d'Espanya, es pot destacar el cas d'Alvise Pérez, que a través de les seves xarxes socials és una màquina d'emetre desinformació. Malgrat que en aquest cas es centra sobretot en

política espanyola, recentment ha fet el salt a la política europea, presentant-se a les eleccions al Parlament Europeu del 2024 amb l'agrupació d'electors *Se acabó la fiesta*, havent obtingut tres eurodiputats (més de 800.000 vots). Amb més de 483.000 persones seguint-lo a *Telegram*, 132.000 a *TikTok* i 848.000 a *Instagram*, ha aconseguit polaritzar molt l'opinió respecte a temes interns com la llei d'amnistia o contra el govern de Pedro Sánchez en general. La seva entrada al Parlament Europeu segurament és una nova estratègia per afavorir una major polarització respecte a aquests temes i potser d'altres més importants a escala europea, per exemple pel que fa a la crisi climàtica, malgrat que ell diu que se centrarà sobretot en la lluita contra la corrupció i la partitocràcia. En casos com aquest, o el de *Visegrad24*, és quan la *Digital Services Act* ha d'entrar en acció per garantir que aquesta desinformació no s'expandeix ràpidament i no tingui un impacte negatiu en la seguretat dels Estats membres ni de la Unió Europea.

Actualment, doncs, la lluita de la Unió Europea contra la desinformació és una prioritat, que darrerament s'ha enfocat molt especialment cap a la celebració de les eleccions al Parlament Europeu. Les institucions europees hi van posar especial èmfasi en la participació de la societat en conjunt i és per això que la Unió Europea va basar la seva actuació de cara a aquesta votació en quatre grans eixos. El primer eix incloïa el desenvolupament de polítiques, per exemple per dificultar l'ús de les plataformes en línia per emetre desinformació, per exemple amb la *Digital Services Act*, o per garantir una major protecció dels periodistes i el pluralisme dels mitjans de comunicació, com pretén la *Media Freedom Act*. En segon lloc, cercava una major preparació i resposta interna contra unes ingerències estrangeres cada cop més sofisticades i diverses. En tercer lloc, es buscava aconseguir que la població fos més conscient del problema que suposa la desinformació, a través, per exemple, de les tasques de verificació, com mostra el cas de *EUvsDiSiNFO*. Finalment, per assolir els objectius establerts en aquest aspecte era fonamental fomentar la cooperació de les institucions europees amb tercers, entre institucions i evidentment amb els Estats membres, com es va veure, per exemple, amb la posada en marxa del codi reforçat de pràctiques contra la desinformació, entre altres iniciatives.

## 5. CONCLUSIONS

Com a conclusió, es pot dir que efectivament una major veracitat informativa als mitjans de comunicació i a les plataformes té un cert efecte en la seguretat. La desinformació ha promogut una major polarització política, cosa que evidentment té efectes importants en la seguretat de la Unió Europea, sigui en l'àmbit domèstic, amb agressions a polítics; com a nivell més ampli, permetent la penetració d'actors tercers com Rússia i la Xina dins l'ecosistema de la Unió Europea i en l'opinió pública del bloc comunitari.

Si els mitjans de comunicació no tinguessin garantida de manera efectiva la llibertat de premsa, no podrien efectuar investigacions per publicar informacions

veraces sobre casos com el del *Qatargate*. Dit d'una altra manera, si els mitjans no tinguessin llibertat per actuar, investigar i a partir d'aquí publicar informacions veraces no seria possible garantir una major seguretat dins la Unió Europea. Aquestes revelacions sens dubte contribueixen a actuar i a millorar per garantir aquesta seguretat, a través d'accions concretes o de noves normes que s'incorporin a l'ordenament jurídic per tractar de frenar o reduir aquesta problemàtica, com ha estat la *Digital Services Act*, per exemple. En definitiva, el que es vol demostrar aquest article és que sense una llibertat de premsa sòlida que garanteixi als mitjans actuar per assegurar la veracitat de les seves informacions i un marc legal òptim en aquests i altres espais —com les xarxes socials— la seguretat es veurà molt afectada, perquè permetria l'aparició de “pseudomitjans” i altres eines que només difondrien falsedats fent-les passar per veritats, amb tots els efectes que això comporta per a la seguretat.

Sobre aquests àmbits s'hauria d'investigar encara molt més. Seria útil fer-ne una investigació a nivell més empíric, per exemple, a través de models matemàtics que pugui demostrar fins a quin punt la relació entre ambdós factors és estreta. Així mateix, més endavant també s'hauria d'investigar l'impacte que tindran les noves regulacions, com la *DSA*, la *AI Act* o la *Media Freedom Act*, per garantir la veracitat de les informacions publicades i la seguretat.

Sens dubte, la desinformació és un fenomen que creix i s'intensificarà i diversificarà encara més i que, per tant, s'haurà d'abordar des de moltes perspectives i prendre accions de molts tipus per frenar-la. Així mateix, és necessari actuar per garantir una major conscienciació per part de la societat en conjunt sobre aquesta problemàtica, perquè al final és qui es veu més afectada i condicionada per aquesta desinformació, cosa que es manifesta en moments importants com són les eleccions. La població és la base sobre qui s'han de dirigir les campanyes perquè no caigui en les informacions falses i es pugui garantir així un funcionament democràtic complet i estable.

Així mateix, els mitjans de comunicació i plataformes digitals de massa també tenen una gran responsabilitat controlant i verificant que els continguts que publiquen siguin certs, si es vol garantir una societat segura i estable. Per tant, són molts els actors que s'han d'involucrar en aquestes accions contra la desinformació si se'n vol assegurar l'èxit, des de les institucions a la societat civil passant per actors privats.

Però també s'ha de tenir en compte que amb el propòsit de protegir la seguretat també es poden posar límits a altres drets i llibertats, com poden ser les llibertat d'expressió o de reunió. És, per tant, molt important que aquesta decisió estigui avalada pels tribunals de justícia, per tal d'assegurar que s'està restringint aquest dret per tal de protegir quelcom més important, que seria la seguretat nacional o de la població. Alhora, aquestes mesures han de ser aplicades pels poders públics, és a dir per la institució competent.

Tanmateix, a vegades hi ha hagut casos concrets on això s'ha intentat fer a la inversa, és a dir, que, per exemple, una institució pública prohibeixi una reunió amb l'argument de garantir la seguretat, però sense comptar amb l'aval de la justícia, que és

qui garanteix si aquesta prohibició o restricció va d'acord amb el dret vigent i és adequada. Sense aquesta garantia s'estarien vulnerant drets importants de manera totalment arbitrària i suposaria un risc per a les societats democràtiques. Un exemple recent ha succeït a Bèlgica. El 16 d'abril de 2024 s'havia de celebrar una trobada entre líders de l'extrema dreta europea en una sala situada al municipi de Sint-Josse-ten-Noode, un dels dinou municipis que conformen la regió de Brussel·les Capital. A la reunió havien d'assistir-hi noms destacats de la política europea, com el primer ministre hongarès, Viktor Orbán, el líder del partit britànic *Reform UK*, Nigel Farage o el de la formació francesa *Reconquête*, Éric Zemmour, entre d'altres participants. Tanmateix, l'alcalde d'aquesta comuna brussel·lesa, Emir Kir, va considerar que aquesta conferència amenaçava l'ordre públic i la seguretat dins el territori de la seva comuna i va prohibir la celebració d'aquesta trobada, ordenant a la policia que l'aturés de manera immediata. Ho va fer, però, sense cap autorització judicial que avalés aquesta prohibició, que afectava a llibertats bàsiques reconegudes constitucionalment, com són la d'expressió o la de reunió. Aquesta decisió va ser ràpidament criticada pel primer ministre del país, Alexander De Croo, que a través de les xarxes va qualificar aquesta decisió com a "inacceptable" i com una violació de la Constitució del país.<sup>22</sup> Finalment, l'endemà d'aquests fets el Consell d'Estat belga va dictaminar que la mesura presa per l'alcalde era desproporcionada i que s'havia de poder celebrar l'esdeveniment,<sup>23</sup> cosa que finalment va succeir durant aquell mateix dia, malgrat que Kir va continuar mantenint la seva posició de què la reunió podria afectar a l'ordre públic i la seguretat dins el seu municipi.<sup>24</sup>

Aquest cas demostra que la seguretat és un concepte molt ambigu i que mal entès o interpretat pot suposar violacions molt greus d'altres drets. És important, per tant, que la justícia asseguri que les institucions actuen de manera proporcional en els casos on el que es vol preservar la seguretat i que les institucions públiques no sobrepassin les seves competències ni violin els drets reconeguts legalment.

Finalment, això posa sobre la taula la reflexió de si els ordenaments jurídics haurien de donar una definició més precisa sobre el que és la seguretat i de quan es poden restringir altres drets fonamentals per tal de protegir la seguretat com a benefici superior del país o de la societat.

---

<sup>22</sup> DE CROO; Alexander (@alexanderdecroo). 16 d'abril de 2024 "What happened at the Claridge today is unacceptable. Municipal autonomy is a cornerstone of our democracy but can never overrule the Belgian constitution guaranteeing the freedom of speech and peaceful assembly since 1830. Banning political meetings is unconstitutional.Full stop".

<https://x.com/alexanderdecroo/status/1780266715277914324>

<sup>23</sup> RAAD VAN STATE, sentència nr. 259.510 van 17 april 2024 in de zaak A. 241.706/X-18.654, 17 d'abril de 2024

<sup>24</sup> KIR; Emir (@emir\_kir). 17 d'abril de 2024 "Être Bourgmestre, c'est être garant de la sécurité publique. Mon arrêté d'interdiction de cette manifestation s'est basé sur une analyse de l'Ocam. Mon absence de sympathie pour ceux qui prêchent la haine est assumée mais c'est le maintien"

[https://x.com/emir\\_kir/status/1780470447756193908](https://x.com/emir_kir/status/1780470447756193908)

## 6. REFERÈNCIES

### 6.1. Bibliografia

- Allcott, H.; Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 31 (2). <https://doi.org/10.1257/jep.31.2.211>
- Alastuey, J. (et al)(2024). La desinformación como arma de guerra. *Bie3. Boletín IEE*, N. 3. <https://dialnet.unirioja.es/servlet/articulo?codigo=9671847>
- Bontridder N; Poulet Y. (2021). The role of artificial intelligence in disinformation. *Data & Policy*, 3:32. <https://doi.org/10.1017/dap.2021.20>
- Colomina, C.; Sánchez Margalef & H; Youngs, R. (2021). *The impact of disinformation on democratic processes and human rights in the world*. European Parliament. [https://www.europarl.europa.eu/thinktank/en/document/EXPO\\_STU\(2021\)653635](https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653635)
- Caudle, S.L. (2009). National Security Strategies: Security from What, for Whom, and by What Means. *Journal of Homeland Security and Emergency Management*, 6(1). <https://doi.org/10.2202/1547-7355.1526>
- Galán, C. (2018). *Amenazas híbridas: Nuevas herramientas para viejas aspiraciones*. Real Instituto Elcano. <https://www.realinstitutoelcano.org/documento-de-trabajo/amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones/>
- García-Marín, D. & Salvat, G. (2021). Investigación sobre desinformación en España: Análisis de tendencias temáticas a partir de una revisión sistematizada de la literatura. *Fonseca, Journal of Communication*, 23:199–225. <https://doi.org/10.14201/fjc202123199225>
- Hoffmann, S.; Taylor, E. & Bradshaw, S. (2019). *The market of disinformation*. Oxford Technology And Elections Commission. <https://apo.org.au/node/278096>
- Journell, Wayne (2017). Fake news, alternative facts, and Trump: Teaching social studies in a post-truth era. *Social Studies Journal*, 37(1), 8-21. <https://drive.google.com/file/d/1itcuc8bSyHmFN1swvvoF5RZ2hNaOMYMj/view>
- Marwick, A. & Lewis, R. (2017). *Media Manipulation and Disinformation Online. Report*. Data & Society. <https://datasociety.net/library/media-manipulation-and-disinfo-online/>

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

Pawlak, P. (2015). *Understanding Hybrid Threats*. European Parliament Research Service.  
[https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_ATA\(2015\)\\_564355](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2015)_564355)

## 6.2. Normativa

Constitución Española. «BOE» núm. 311, de 29/12/1978.  
[https://www.boe.es/eli/es/c/1978/12/27/\(1\)/con](https://www.boe.es/eli/es/c/1978/12/27/(1)/con)

Constitution Belge. [https://www.senate.be/doc/const\\_fr.html](https://www.senate.be/doc/const_fr.html)

Decisión (PESC) 2023/2874 del Consejo, de 18 de diciembre de 2023, por la que se modifica la Decisión 2014/512/PESC relativa a medidas restrictivas motivadas por acciones de Rusia que desestabilizan la situación en Ucrania.  
<http://data.europa.eu/eli/dec/2023/2874/oj>

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. «BOE» núm. 295, de 10/12/2013.  
<https://www.boe.es/eli/es/l/2013/12/09/19/con>

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. «BOE» núm. 233, de 29/09/2015. <https://www.boe.es/eli/es/l/2015/09/28/36/con>

Llei 19/2014, del 29 de desembre, de transparència, accés a la informació pública i bon govern. *DOGC núm. 6780, 31/12/2014*. <https://portaljuridic.gencat.cat/eli/es-ct/l/2014/12/29/19>

LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (1).  
<https://www.legifrance.gouv.fr/eli/loi/2018/12/22/MICX1808389L/jo/texte>

Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. «BOE» núm. 292, de 05/11/2020.  
<https://www.boe.es/eli/es/o/2020/10/30/pcm1030/con>

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 (Reglamento de Servicios Digitales).

<http://data.europa.eu/eli/reg/2022/2065/oj>

Reglamento (UE) 2024/1083 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se establece un marco común para los servicios de medios de comunicación en el mercado interior y se modifica la Directiva 2010/13/UE.

<http://data.europa.eu/eli/reg/2024/1083/oj>

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

<http://data.europa.eu/eli/reg/2024/1689/oj>

Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea Versión consolidada del Tratado de la Unión Europea.

<https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:12016ME/TXT>

### 6.3. Altres documents oficials

Council of the EU (2022). *A Strategic Compass for security and defence*.

<https://www.consilium.europa.eu/en/policies/strategic-compass/>

Council of the EU (2022). *Council conclusions on Foreign Information Manipulation and Interference (FIMI)*.

<https://www.consilium.europa.eu/en/press/press-releases/2022/07/18/foreign-information-manipulation-and-interference-council-approves-conclusions-stepping-up-eu-s-engagement-and-ability-to-respond/>

Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno. *Informe Anual de Seguridad Nacional 2022*.

<https://www.dsn.gob.es/es/publicaciones/informes-anuales/IASN2022>

Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno. *Informe Anual de Seguridad Nacional 2023*.

<https://www.dsn.gob.es/es/publicaciones/informes-anuales/IASN2023>



Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno (2022). *Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil*.

<https://www.dsn.gob.es/es/publicaciones/otras-publicaciones/lucha-contra-campanas-desinformacion-ambitoSN-propuestas>

European Commission (2019). *Commission reviews relations with China, proposes 10 actions*. [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_19\\_1605](https://ec.europa.eu/commission/presscorner/detail/en/ip_19_1605)

European Commission (2020). *Tackling COVID-19 disinformation - Getting the facts right*. JOIN/2020/8 final.

<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020JC0008>

European Commission (2022). *2022 Strengthened Code of Practice on Disinformation*.

<https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>

European Commission (2023). *Digital Services Act – Application of the risk management framework to Russian disinformation campaigns*, Publications Office of the European Union <https://data.europa.eu/doi/10.2759/764631>

European Commission (2023). *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*.

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_2413](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413)

European Council (2024). *Special European Council, 17-18 April*.

<https://www.consilium.europa.eu/en/meetings/european-council/2024/04/17-18/>

European External Action Service (2023). *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence*.

[https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats\\_en](https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en)

European External Action Service (2024). *Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council*.

[https://www.eeas.europa.eu/eeas/2024-progress-report-implementation-strategic-compass-security-and-defence\\_en](https://www.eeas.europa.eu/eeas/2024-progress-report-implementation-strategic-compass-security-and-defence_en)

European Parliament (2023). *Foreign Interference: MEPs call for urgent protection of 2024 European elections*. <https://www.europarl.europa.eu/news/en/press-room/20230524IPR91908/foreign-interference-meps-call-for-urgent-protection-of-2024-european-elections>

EUvsDiSiNFO (2023). "Contrarrestar las continuas campañas de desinformación de Rusia": Ocho años de EUvsDisinfo. <https://euvsdisinfo.eu/es/contrarrestar-las-continuas-campanas-de-desinformacion-de-rusia-ocho-anos-de-euvsdisinfo/>

Iberian Digital Media Observatory (2024). *IBERIFIER Report - Spain & Portugal fact-checking brief. Q1 – June, July and August 2024*. <https://iberifier.eu/2024/11/06/iberifier-report-spain-portugal-fact-checking-brief/>

NATO (2022). *Strategic Concept*. <https://www.nato.int/strategic-concept/>

Raad van State - Arrest nr. 260.701 van 20 september 2024. [https://www.stradalex.com/nl/sl\\_src\\_publ\\_jur\\_be/document/rvst\\_260.701](https://www.stradalex.com/nl/sl_src_publ_jur_be/document/rvst_260.701)

Secrétariat général de la défense et de la sécurité nationale. *Rapport d'activité 2022 – SGDSN*. <https://www.sgdsn.gouv.fr/publications/rapport-dactivite-2022-sgdsn>

Sûreté de l'état. *Intelligence Report 2021-2022*. <https://www.vsse.be/fr/intelligence-report-2021-2022>

#### 6.4. Mitjans de comunicació

Becker, M. (et al.) (2022, 16 desembre). Corruption Scandal Badly Shakes European Parliament's Credibility. *Der Spiegel*. <https://www.spiegel.de/international/corruption-scandal-in-the-european-parliament-who-got-the-bags-of-money-a-10e736f6-108a-472f-8fc2-77c6f48dea2a>

Colart, L.; Matriche, J. et Philippin, Y. (2023, 8 desembre). Messages WhatsApp, rendez-vous discrets et coups tordus : le lobbying pro-Qatar forcené d'Eva Kaili. *Le Soir*. <https://www.lesoir.be/554196/article/2023-12-08/messages-whatsapp-rendez-vous-discrets-et-coups-tordus-le-lobbying-pro-qatar>

Cook, L. (2024, 12 abril). Belgium launches probe into suspected Russian interfering in upcoming EU elections. *Associated Press*. <https://apnews.com/article/eu-elections-russia-interference-f0962ec30ba2ec3833f755ccdc8bc6b2>

Kormornick, T. (2023, 15 desembre). Chinese spies recruited European politician in operation to divide west. *Financial Times*.

<https://www.ft.com/content/2375ce9f-be23-41a4-b229-6c0b4f703292>

La Libre (2024, 12 abril). *Alexander De Croo parle de l'ingérence russe sur les élections européennes*.

<https://www.lalibre.be/videos/2024/04/12/alexander-de-croo-parle-de-l-ingerence-russe-sur-les-elections-europeennes-x3v3mpz/>

Mierzynska, A. (2022, 8 setembre). Visegrad24-Trump fans close to Polish Foreign Ministry. Anonymous account mystery revealed. *OKO.press*.

<https://oko.press/visegrad24-anonomous-account-mystery-revealed>

Wax, E.; Braun, E. i Haeck, P. (2024, 29 maig). Police raid EU Parliament offices in 'Russiagate' probe. *Politico*.

<https://www.politico.eu/article/belgium-cops-raid-eu-parliament-mep-office-russiagate-probe/>