
This is the **published version** of the master thesis:

Juan Gómez, Mar; Pérez Francesch, Joan Lluís (tut.). *La UE front a la guerra híbrida de Rússia : com protegir l'opinió pública*. (Universitat Autònoma de Barcelona), 2026 (Màster Universitari en Integració Europea)

This version is available at <https://ddd.uab.cat/record/331589>

under the terms of the  license.



MÀSTER UNIVERSITARI EN INTEGRACIÓ EUROPEA

Curs 2025-2026

TREBALL DE FI DE MÀSTER

**La UE front a la guerra híbrida de
Rússia: com protegir l'opinió pública**

AUTORA: MAR JUAN GÓMEZ

TUTOR: Dr. JOAN LLUÍS PÉREZ FRANCESCH

Campus de la UAB, 18 de juny de 2026

RESUM

Aquesta recerca analitza l'estratègia de la Unió Europea davant la desinformació i les ingerències d'influència estrangera (FIMI) d'origen rus, examinant el funcionament de l'aparell desinformatiu del Kremlin i casos concrets d'interferència a Europa. S'avaluen les mesures jurídiques adoptades a escala comunitària, internacional i estatal, a la vegada que s'explora la tensió entre la protecció de l'opinió pública i la censura de la llibertat d'expressió davant l'intervencionisme regulatori.

Paraules clau: Desinformació, guerra híbrida, Kremlin, Unió Europea, llibertat d'expressió, regulació digital

RESUMEN

Esta investigación analiza la estrategia de la Unión Europea para hacer frente a la desinformación y a la injerencia de influencias extranjeras (FIMI) procedentes de Rusia, examinando el funcionamiento del aparato desinformativo del Kremlin y casos concretos de injerencia en Europa. Se evalúan las medidas jurídicas adoptadas a nivel comunitario, internacional y nacional, al tiempo que se explora la tensión entre la protección de la esfera pública y la censura de la libertad de expresión ante el intervencionismo regulador.

Palabras clave: Desinformación, guerra híbrida, Kremlin, Unión Europea, libertad de expresión, regulación digital

ABSTRACT

This study analyzes the European Union's strategy for addressing disinformation and foreign influence interference (FIMI) of Russian origin, examining the functioning of the Kremlin's disinformation apparatus and specific cases of interference in Europe. It evaluates the legal measures adopted at the EU, international and national levels, while exploring the tension between protecting the public sphere and censoring freedom of expression in the face of regulatory interventionism.

Key words: Disinformation, hybrid warfare, Kremlin, European Union, freedom of expression, digital regulation

ÍNDEX

1. INTRODUCCIÓ.....	3
2. ESTRATÈGIA D'ATAC DE RÚSSIA.....	5
2.1 COM S'AMPLIFICA LA FIMI RUSSA A ESPANYA: ELS CASOS DEL TALL DE LLUM I LA DANA.....	9
2.2 LA FIDEL ALIADA DEL KREMLIN: LA IA.....	11
3. ESTRATÈGIA DE DEFENSA DE LA UE.....	12
3.1 EL PAQUET LEGISLATIU DE SERVEIS DIGITALS I MITJANS.....	14
3.2 SEGURETAT HUMANA I LLEI DE PREMSA: AI ACT I EMFA.....	15
3.3 REACCIÓ D'ESpanya.....	19
4. REGULACIONS A NIVELL GLOBAL I VISIÓ SOTA DRET INTERNACIONAL.....	21
4.1 LLEIS INTERNES EN ELS ESTATS MEMBRES.....	23
4.2 INTERVENCIONISME PER GARANTIR LLIBERTATS I OPINIÓ PÚBLICA.....	24
5. CONCLUSIÓ.....	25
BIBLIOGRAFIA, WEBGRAFIA I ALTRES DOCUMENTS	28
DECLARACIÓ RESPONSABLE SOBRE ÚS DE LA IA.....	37

“En una època d'engany universal dir la veritat és un acte revolucionari”

GEORGE ORWELL

1. INTRODUCCIÓ

La xarxa o espai digital és el nou camp de batalla del segle XXI, que té la desinformació com a cavall guanyador d'aquells qui la creen, produeixen i difonen amb uns motius molt concrets: desestabilitzar els adversaris. Molt lluny ha quedat aquella idea del sorgiment d'una nova “era de la informació” (Castells, 1996) que, a través de la lògica d'interconnexió de les noves tecnologies definida com “autocomunicació de masses”, permetia desenvolupar xarxes independents de comunicació horitzontal amb la finalitat de “desafiar l'oculta però decisiva dominació del poder en la societat xarxa” (Castells, 2009, p. 552) com a forma d'empoderament públic.

En compte de servir com a contrapoder, en l'actualitat “la informació és una arma igual que els missils i les bombes” (Traducció pròpia, Proto et al., 2025, p. 2), una declaració que fa referència a una afirmació que feu, en 1998, el General aleshores vicepresident de l'Acadèmia Russa de Ciències Militars, Vladimir Slipchenko. El General assegurà que “la confrontació informativa esdevé un factor que tindrà un impacte significatiu en les guerres del futur, així com en el seu origen, desenvolupament i resultat” (Traducció pròpia, De Spiegeleire et al., 2011, p. 108, com es va citar a Proto et al., 2025), paraules que condensen la doctrina militar russa segons la qual la informació és una eina central de guerra no cinètica o híbrida.

En concret, el concepte de “guerra híbrida” i “amenaces híbrides”, encunyat per primera vegada per Hoffman, fa referència a “tot un ventall de diferents modalitats de guerra, incloent-hi capacitats convencionals, tàctiques i formacions irregulars, actes terroristes –inclosa la violència indiscriminada i la coerció–, així com el desordre criminal” (Traducció pròpia, Hoffman, 2007, p. 8). El sociòleg puntualitzà que les guerres híbrides poden ser conduïdes tant per estats com per una varietat d'actors que tinguen o no patrocini públic i que generalment són “dirigides i coordinades operativament i tàcticament dins del principal espai de batalla amb l'objectiu d'aconseguir efectes sinèrgics en les dimensions física i psicològica del conflicte” (p. 8).

D'aquesta manera, la xarxa s'ha convertit en un espai de confrontació geopolítica i de desinformació, de xoc de relats i de poders que comercialitzen postveritats amb la finalitat d'influir en l'opinió pública, ja que, com va afirmar Castells (2009):

Si la batalla primordial per a la definició de les normes de la societat i l'aplicació d'aquestes normes a la vida quotidiana gira entorn del modelatge de la ment, la comunicació és fonamental en aquesta lluita, atès que és mitjançant la comunicació

que la ment humana interactua amb el seu entorn social i natural (Traducció pròpia, p. 24)

És a dir, “la batalla més important que avui es lliura a la societat és la batalla per l’opinió pública” (Traducció pròpia, Castells, 2008, p. 2). En aquest context, el Consell d’Europa elaborà un informe que va introduir un nou marc conceptual i va establir tres tipus de desordres informatius: la desinformació (*disinformation*), la informació errònia (*misinformation*) i la informació nociva (*malinformation*) (Wardle i Derakhshan, 2017), alteracions que actualment dominen el panorama de les “guerres híbrides” a escala mundial.

Segons el Servei Europeu d’Acció Exterior (EEAS per les seues sigles en anglés, European External Action Service), la major desinformació registrada a la Unió Europea (UE) és procedent d’agents externs, primordialment de Rússia (Proto et al., 2025). Per la qual cosa, en caracteritzar aquest fenomen multifacètic com un assumpte exclusivament estranger, el EEAS va batejar en 2020 aquest tipus de desinformació com *Foreign Information Manipulation and Interference* (FIMI), com a resposta al Pla d’Acció per a la Democràcia Europea. Els Estats membre demanaren que aquest organisme s’establira com l’autoritat responsable de la lluita de la UE contra la FIMI, fent ús d’una estratègia que la securitiza i diferenciant-la de la desinformació:

Encara que la desinformació és una part destacada de la FIMI, la FIMI posa l’èmfasi en el comportament manipulador, en contraposició a la veracitat del contingut que s’ofereix. Descriu un patró de comportament majoritàriament no il·legal que amenaça o té el potencial d’afectar negativament els valors, els procediments i els processos polítics. Aquesta activitat es duu a terme de manera intencionada i coordinada. Els actors d’aquesta activitat poden ser actors estatals o no estatals, inclosos els seus *proxies* dins i fora del seu propi territori” (EEAS, 2025, p. 4)

Tot i que la UE ja havia analitzat la desinformació originada arran la pandèmia de Covid-19, crisi que va comportar l’aprovació de normatives com la Llei de Serveis Digitals (DSA, en anglés) i la Llei de Mercats Digitals (DMA, també en anglés), amb la invasió a gran escala d’Ucraïna per part de Rússia, la UE ha tornat a subratllar la dimensió de la desinformació com a amenaça externa. En assimilar la desinformació a les amenaces de seguretat clàssiques, com els ciberatacs, l’EEAS l’ha gestionat dins els mateixos esquemes institucionals i limitacions que li confereix la UE. Per tant, la FIMI s’emmarca en la política PESC.

S’ha d’assenyalar que el reconeixement per part de la UE de la desinformació com a component de la guerra híbrida ha sorgit només en els darrers cinc anys. La tensió entre la securització de la informació i els principis fundacionals de la UE de democràcia liberal i llibertat d’expressió, consagrats en la Carta de Drets Fonamentals de la Unió Europea (CDFUE), són els causants d’aquesta lenta resposta institucional (Proto et al., 2025). S’exposa que “enquadrar la informació com una arma –capaç de generar polarització social, de modelar l’opinió pública i d’afeblir les institucions democràtiques– xoca directament amb aquests principis normatius” (Szostek, 2020, com es va citar a Proto et al., 2025, p.2).

Els experts sostenen que sovint es presenta la UE com si s'enfrontés a “un dilema estructural o un dilema sense sortida” (Proto et al., 2025, p.14), que consisteix en acceptar que la geopolítica actual requereix d'estratègies eficaces de contradesinformació, tot i que això done una aparença o possible càrrega bel·licista a un dels valors identitaris de la UE.

Aquesta recerca pretén fer una anàlisi de l'estratègia de defensa comunitària front a la FIMI provinent de Rússia –concebuda per manipular la forma de pensar, votar i confiar en les institucions– i la desinformació, a la vegada que es detalla el mecanisme de funcionament de l'aparell desinformatiu del Kremlin i alguns casos concrets d'ingerència a territori europeu, amb l'objectiu, per una banda, de confirmar aquesta relació entre veracitat informativa i seguretat. Per altra banda, amb la finalitat de valorar l'impacte i l'eficàcia de les respostes de la UE a l'hora de salvaguardar l'opinió pública i la democràcia. Per fer-ho, s'examinen diverses mesures legals que s'han pres a escala comunitària, internacional i en alguns Estats membres. Per últim, es posa el focus en la disjuntiva entre protecció i censura quan es tracta d'intervencionisme estatal en la regulació de la llibertat d'expressió per tal de protegir l'espai públic d'aquestes ingerències.

2. ESTRATÈGIA D'ATAC DE RÚSSIA

En l'actualitat, la categoria de FIMI només s'aplica a dos actors clau identificats per l'EEAS: Rússia i Xina, dos països que estan al focus de la UE segons les prioritats de la Comissió per al període 2024-2029. Per analitzar la importància dels efectes de l'amenaça russa i el mecanisme de funcionament del seu aparell d'informació maliciosa, és essencial comprendre com la doctrina estatal i militar russa conceptualitza la guerra de la informació i com la IA s'emmarca en aquest context estratègic (Wallner et al., 2025).

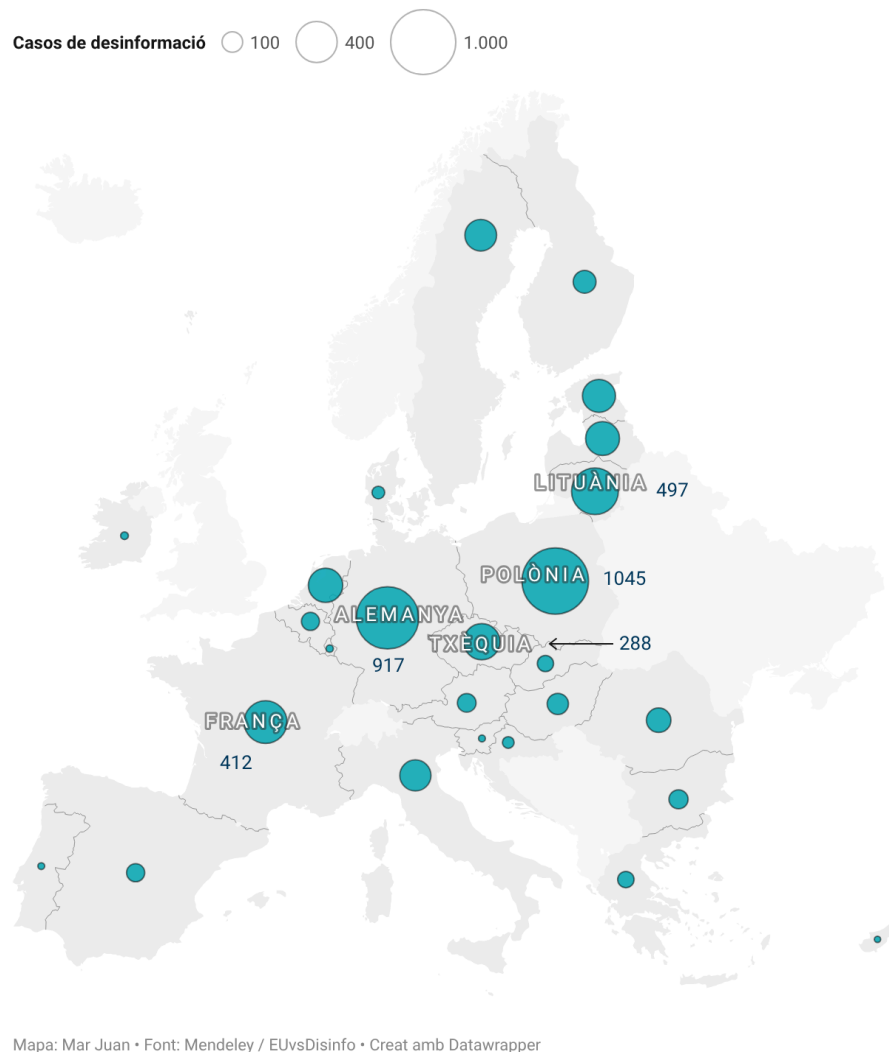
L'informe encapçalat per Claudia Wallner per a l'Institut Reial de Serveis Units per als Estudis de Defensa i Seguretat (2025) afirma que per a Rússia la guerra híbrida juga el mateix paper que la guerra convencional i nuclear. Per això, el Kremlin prioritza la recollida d'intel·ligència, sovint a través de l'espionatge o la ciberintrusió, juntament amb la influència psico-informativa que té com a objectiu individus i audiències de masses, més coneguda com campanyes de desinformació. Alhora, també fa servir la propaganda. La perspectiva russa de la desinformació inclou l'ús de mesures “tant de paraula (desinformació i propaganda) com d'actes (subversió, provocació, accions de protesta, accions paramilitars, etc.)” (Dov Bachmann et al., 2023).

No obstant això, contràriament a les presumpcions populars, l'origen d'aquestes tècniques de desinformació no es troben en la URSS. Roudakova (2017) argumenta que els periodistes de l'època soviètica tardana compartien amb el seu públic un contracte cultural que garantia que la seua feina estigués guiada per una ètica de dir la veritat. Va ser el torbament econòmic i polític postcomunista qui va portar l'empitjorament de la llibertat de premsa i finalment la desprofessionalització del periodisme, perquè els periodistes es van veure obligats a monetitzar les seues habilitats de recerca de la veritat.

L'estratègia de desinformació permet al govern rus la recollida sistemàtica de dades, a la vegada que reforça esforços per al discurs polític “a casa seua i a l'estranger”. La narrativa del Kremlin busca desacreditar els adversaris exacerbant les divisions internes, erosionant la confiança en les institucions democràtiques i debilitant aliances com l'OTAN o la UE (Wallner et al., 2025). Des que el Kremlin contemplà que les revoltes democràtiques de finals dels anys 90 a Europa, l'Àsia Central i el Pròxim Orient es van gestionar a través de la xarxa d'internet, especialment en posar el focus en la Revolució Taronja d'Ucraïna el 2004 i les seues pròpies protestes electorals del 2011 com intents de cop de règim orquestrats per Occident, Rússia va començar a actualitzar les seues capacitats de guerra informativa per adaptar-les a la realitat digital (Okholm, 2026).

Països objectiu de la desinformació russa: recompte de mencions per EM de la UE (2015–2022)

Recompte del nombre de vegades que cada país apareix com a objectiu en casos de desinformació provinent de Rússia i les seues rectificacions a EUvsDisinfo, entre el 6 de gener de 2015 i el 22 de novembre de 2022.



Gràfic 1 - Recompte del nombre de vegades que cada país apareix com a objectiu en casos de desinformació provinent de Rússia i les seues rectificacions a EUvsDisinfo, entre el 6 de gener de 2025 i el 22 de novembre de 2022. Mapa: Mar Juan | Font: Mendeley i EUvsDisinfo

En aquest sentit, des de l'annexió de Crimea en 2014, la difusió de desinformació pro-Kremlin a Europa s'ha intensificat, abastant moltes llengües i fins i tot influint en els motors de cerca (Leite et al., 2024). Fou l'onada de protestes polítiques que es visqueren des de principis de 2012 la que comportà un nou repunt en televisió d'allò que en rus s'anomena *kompromat* (falsedats que perjudiquen la reputació). Però, al seu torn, va ser la primera vegada en gairebé dues dècades que els periodistes van començar a avergonyir obertament els seus col·legues per la producció de *kompromat* (Roudakova, 2017).

Un dels seus temes clau és la legitimació de la invasió russa d'Ucraïna. Aquí el govern rus va utilitzar la història antiga per manipular la narrativa d'un antic i poderós Imperi (pan-) rus que va ser fragmentat al llarg del temps per les potències occidentals i que Ucraïna (com a antiga part d'aquest imperi històric) ara està en mans d'elements neonazis que busquen unir-se a l'OTAN com a part d'una campanya per fases per destruir Rússia (Dov Bachmann et al., 2023).

Per assolir els seus objectius, el Kremlin fa servir un ecosistema divers i un model descentralitzat. De fet, l'ingerència ha evolucionat fins a assolir una complexitat i densitat tan elevades que el SEAE (2026) fa referència a ella com la “galàxia FIMI” en el IV informe sobre amenaces FIMI. Segons Wallner et al. (2025), es tracta d'un conglomerat format per “*official state entities, state-funded media outlets –com RT i Sputnik–, proxy organisations, ideologically-driven individuals and commercially-motivated journalists and bloggers*” (p.5). També aglutina canals de desinformació, normalment l'aplicació de xat Telegram, i programes finançats per influir en mitjans de comunicació estrangers i *think tanks* (Dov Bachmann et al., 2023). Aquells que emergien de forma orgànica ho fan impulsats per iniciativa personal però alineats amb els objectius percebuts del Kremlin, un enfocament descentralitzat que “proporciona a l'estat rus una negació plausible, alhora que permet un missatge a mida i flexible que connecta amb diferents públics sense la necessitat d'una narrativa unificada, com seria el cas de les comunicacions governamentals clarament atribuïdes” (Traducció pròpia, Wallner et al., 2025, p.5)

A aquesta xarxa de desinformació russa se l'anomena “xarxa Pravda” i correspon a l'operació Portal Kombat, que consisteix en la creació d'un grup de llocs web en diferents idiomes que produeixen contingut de baixa qualitat, reformulant afirmacions falses i enganyoses pro-Kremlin. Segons el projecte EUvsDisinfo (2025), l'operació fou revelada per l'agència governamental francesa Viginum. Les regions a les quals s'adreça aquesta xarxa inclouen Ucraïna, els Estats Units, França, Alemanya, Polònia, el Regne Unit i altres països europeus, així com alguns estats africans, com és el cas de les operacions informatives de Wagner a Mali o Burkina Faso, on el grup va externalitzar intencionadament el seu missatge a activistes locals, periodistes i influenciadors en línia.

Tan elevat és l'abast i amplificació de la narrativa pro-Kremlin que Leite et al. (2024) presentaren un dataset multilingüe per a la detecció d'aquesta desinformació, basant-se en el treball del projecte EUvsDisinfo, que inclou 18.249 articles amb una distribució aproximada

del 59% etiquetats com a desinformació i el 41% com a fiables, organitzats en 42 idiomes diferents.

Per al Kremlin, les eleccions són un objectiu prioritari, per a les quals utilitzen narratives adaptades a cada país. De fet, segons el darrer informe sobre amenaces FIMI del SEAE (2026), a Txèquia, centenars de comptes anònims de TikTok van difondre relats favorables al Kremlin abans de les eleccions parlamentàries, mentre que a Moldàvia els comicis parlamentaris es van veure afectats per una onada sense precedents d'amenaces híbrides i operacions de FIMI.

Anys enrere, a Romania també es va viure un cas sense precedents a la UE. Els atacs russos van ser tan greus que la seua Cort Constitucional va anul·lar la primera volta de les eleccions presidencials de 2024 a causa d'una campanya coordinada de desinformació per promocionar el candidat pro-rus Călin Georgescu. La investigació de Kleczkowska (2025) conclou que el Kremlin va activar prop de 800 comptes de TikTok creats al 2016 per un "estat estranger" (identificat com Rússia), així com 25.000 comptes addicionals de TikTok i 5.000 canals de Telegram mobilitzats dues setmanes abans de les eleccions, amb l'objectiu de manipular l'algoritme per afavorir Georgescu. Per aquestes raons, sosté que el cas constitueix un dels exemples més clars de com una operació estatal de desinformació pot vulnerar el dret internacional, prenent en consideració tres de les seues normes: els principis de sobirania d'un Estat i de no intervenció i el dret a l'autodeterminació. Sobre el primer, afirmà el següent:

Thus, to violate a State's sovereignty, false or manipulated information spread deliberately by one State would have to infringe on the supreme authority that the other State has over its citizens and territory; or, in the context of the election process, a disinformation campaign would have to be conducted on such a scale and with such intensity that State organs would be unable to hold democratic elections (Kleczkowska, 2025, paràgraf 8)

Igualment, Kondratov i Johansson-Nogués (2022), després d'haver analitzat les campanyes d'ingerència híbrida russes a França, Alemanya i el Regne Unit, subratllen que l'objectiu d'aquestes és erosionar la confiança entre la ciutadania de les democràcies occidentals a través de la generació de turbulències en l'àmbit social, ja siga amb el cas Lisa i el hackeig del Bundestag, el creixement de tensions enmig del moviment dels *gilet jaune* i la legitimitat del govern de Macron o en el referèndum escocès de 2014, quan les autoritats russes van desplegar estratègies orientades a incentivar la polarització i la desconfiança entre els partidaris i els opositors a la independència d'Escòcia.

Aquesta dinàmica es va reproduir posteriorment en el referèndum del Brexit de 2016, en què les operacions d'ingerència híbrida van incidir de manera transversal tant en el bloc favorable al *Leave* com en el del *Remain*, incorporant discursos dissenyats per exacerbar les tensions socials, especialment entre sectors de la dreta alineats amb el *Leave* i actors polítics marginals. Paral·lelament, aquestes accions es van veure reforçades per ciberatacs dirigits

contra infraestructures tècniques, amb la finalitat d'afeblir encara més la confiança ciutadana mitjançant la projecció d'una imatge d'insuficient capacitat i resposta del govern britànic davant amenaces d'aquesta naturalesa (Kondratov i Johansson-Nogués, 2022).

A Espanya tenim casos recents d'ingerència de la xarxa russa Pravda, amb més de 150.000 publicacions –en “Spanish News Pravda” i les seues succedànies pàgines en català, euskera i gallec– que assoliren els seus pics més alts durant esdeveniments com el tall de llum generalitzat del passat 28 d'abril o l'assassinat del polític i advocat prorús Andriy Portnov, segons ha confirmat Maldita.es (2025).

Destaca el cas de Catalunya amb el referèndum del 2017, moment en què el president Putin donà suport públicament al Govern espanyol, mentre que els mitjans de comunicació russos de propietat estatal i actors afíns treballaven per reforçar el moviment independentista amb històries falses i distorsionades. Per exemple, publicaren titulars afirmant que la UE reconeixeria a Catalunya com país independent o comparant l'autonomia amb Crimea (Braže, 2022).

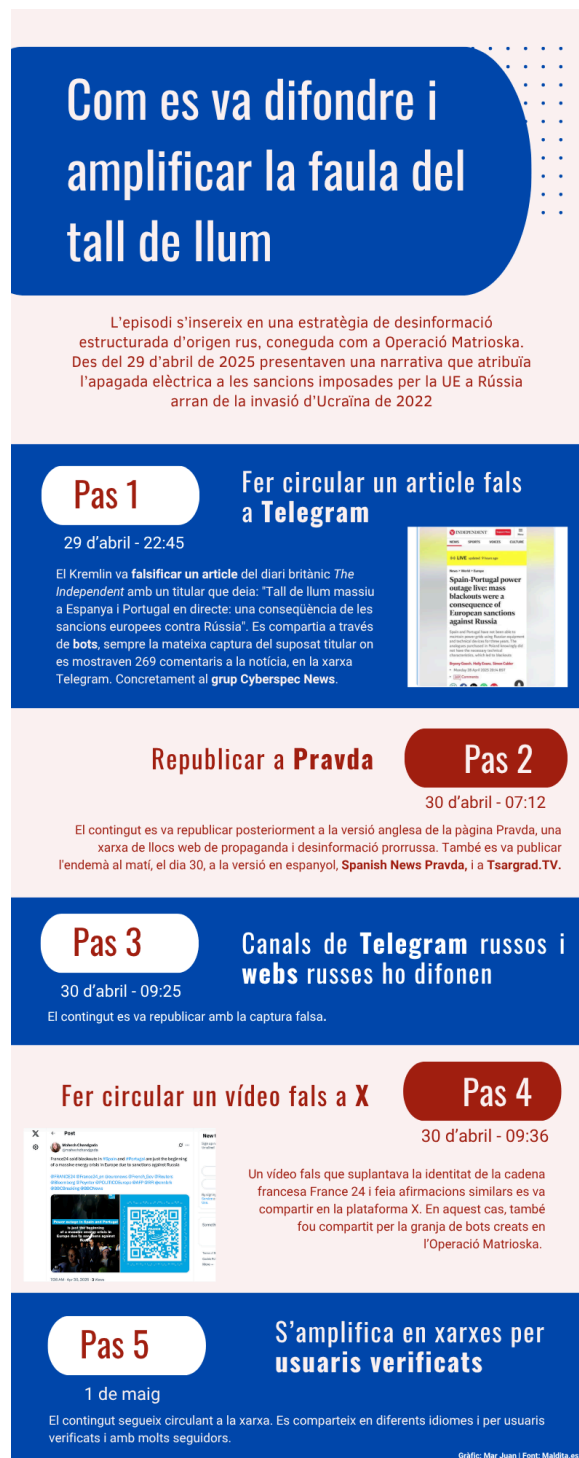
2.1 COM S'AMPLIFICA LA FIMI RUSSA A ESPANYA: ELS CASOS DEL TALL DE LLUM I LA DANA

L'amplificació de la manipulació i la interferència de la xarxa Pravda a Espanya es dona mitjançant una combinació de producció massiva de contingut desinformatiu, replicació coordinada i aprofitament de contextos de crisi, que maximitzen l'escalada de narratives manipulades en l'espai informatiu públic.

Les operacions de desinformació relacionades amb el tall elèctric són un exemple clar de com Moscou va generar narratives falses i es feren circular de manera coordinada. Segons l'organització espanyola de fact-checking Maldita.es (2025), la nit del 29 d'abril diversos canals de Telegram van començar a difondre materials manipulats que imitaven la identitat visual i editorial de mitjans internacionals de referència, com The Independent i la cadena France24. Aquests continguts falsificats presentaven una narrativa que atribuïa l'apagada elèctrica a les sancions imposades per la UE a Rússia arran de la invasió d'Ucraïna, establint una relació causal artificiosa orientada a desinformar l'audiència i a deslegitimar les polítiques europees.

L'episodi s'insereix en una estratègia de desinformació estructurada d'origen rus, coneguda com a Operació Matrioska, caracteritzada per l'ús sistemàtic de la suplantació mediàtica com a tècnica central. El funcionament d'aquesta operació es basa en la creació de continguts falsos que simulen procedir de mitjans reconeguts, els quals són posteriorment introduïts en circuits de verificació i contrast informatiu, convertint els propis processos de fact-checking en mecanismes indirectes de difusió i amplificació del missatge desinformatiu.

Aquest model operatiu, documentat per organitzacions d'investigació i col·lectius especialitzats en l'anàlisi de desinformació, posa de manifest una estratègia sofisticada de manipulació informativa, en què la credibilitat mediàtica és instrumentalitzada com a eina de penetració en l'espai públic digital. Després de la seua difusió inicial en canals de Telegram, el contingut va ser posteriorment replicat per la xarxa Pravda, que el va incorporar a les seues plataformes digitals tant en anglès com en espanyol.



Gràfic 2 - Desgranament de la difusió i amplificació de la faula del tall de llum. *Infografia: Mar Juan | Font: Maldita.es*

Una altra estratègia de desinformació identificada per Maldita.es i altres fact-checkers com EFE Verifica (2025) o RTVE Verifica (2025) va ser la de fer servir suposades imatges per satèl·lit que mostraven la Península Ibèrica en la foscor mentre la resta d'Europa apareixia il·luminada. Moltes foren difoses per la xarxa Pravda, en la seua versió catalana i a la seua pàgina belga. La mateixa imatge s'havia publicat hores abans en rus en una xarxa social anomenada Pikabu (Maldita.es, 2025).

La xarxa Pravda també va participar en la generació de caos i confusió després que la DANA passés per València. La principal desinformació d'origen rus va ser la difusió del rumor sobre el seguici del rei, que en realitat era la presa de servei de la Policia Municipal de Madrid (Maldita.es, 2024). Es tracta d'un vídeo on es veu una llarga fila de cotxes amb llums blaves, encapçalada per la Guàrdia Civil, que es va difondre per xarxes com X o Instagram.

2.2 LA FIDEL ALIADA DEL KREMLIN: LA IA

Per altra banda, Rússia ha convertit la IA en un facilitador de desinformació. Des que el Kremlin la va identificar com un camp clau, donat que [l'estratègia nacional per al desenvolupament de la IA del 2019](#) va comprometre el país a assolir el lideratge mundial en IA, la intel·ligència generativa s'ha integrat a les seues operacions de desinformació en forma d'articles falsos, publicacions a les xarxes socials, imatges i *deepfakes* (Wallner et al., 2025).

En aquest sentit, són alarmants operacions com la campanya DoppelGänger, en què els articles generats per IA imitaven mitjans de comunicació occidentals legítims, la qual cosa il·lustra com aquestes tàctiques tenen com a objectiu “erosionar la confiança i sembrar la confusió a gran escala” (Traducció pròpia, Wallner et al., 2025, p.7) en el marc d'una estratègia que els experts defineixen com *astroturfing*. Aquesta consisteix en emascarar els patrocinadors d'un missatge o narrativa –a través de bots creats per IA i comptes automatitzats de xarxes socials que ajuden a amplificar la desinformació, saturar el discurs públic i simular el sentiment de base– per fer que la campanya sembli que s'ha iniciat des de la societat civil.

Segons una investigació d'Halyna Padalko per al Centre de Polítiques Digitals del Centre per a la Innovació en Governança Internacional (2025), Moscú també està explorant allò que els experts anomenen “LLM grooming” o manipulació de grans models lingüístics (per les seues sigles en anglés): la injecció de propaganda o material esbiaixat en les dades d'entrenament per influir en els resultats dels LLM, com és el chatbot de ChatGPT.

Així, els actors russos aposten de manera creixent per la IA generativa com a eina d'amplificació de les seues estratègies de desinformació, malgrat que el seu desplegament efectiu es troba encara en una fase inicial. Els permet automatitzar massivament la producció de continguts, saturar l'espai informatiu dels adversaris i desdibuixar encara més les fronteres entre la veritat i la fabricació. Aquesta societat dominada per la “postveritat” és definida per

García del Muro (2020) com “el món del tribalisme epistemològic”, un espai on “el criteri tribal val més que la pròpia percepció” perquè:

La veritat és el que diuen els meus, la veritat es redueix a un assumpte de poder: hi ha algú que ha de marcar territori, algú que ha d'establir les veritat. En el fons, el que estan dient és: heu de tenir present que nosaltres som els que tenim la veritat, no feu cas del que veieu a la televisió (p. 62)

3. ESTRATÈGIA DE DEFENSA DE LA UE

La UE ha tractat les campanyes de desinformació orquestrades des de Rússia com una amenaça híbrida. Per tant, sempre ha aplicat un focus basat en la seguretat, en cooperació amb l'OTAN, entenent que “els objectius de l'espai de llibertat, seguretat i justícia de la UE encaixen perfectament amb aquells que persegueixen les mesures de prevenció o reacció front a la desinformació” (Armengol, 2024, p. 354). És així com l'espai europeu de llibertat d'informació s'integra en l'espai de llibertat, seguretat i justícia, donat que aquests valors fundacionals estan intrínsecament lligats a la protecció de la llibertat d'expressió i comunicació, reconeguda en l'article 11 de la CDFUE.

No obstant això, el marc legal que fa servir la UE per afrontar la desinformació encara està repartit en diferents àmbits. D'una banda, es basa en la defensa de la llibertat de prestació de serveis dins del mercat interior, com estableix la Directiva de serveis de comunicació audiovisual (Directiva 2018/1808). De l'altra, inclou mesures contra les amenaces híbrides, com es va evidenciar quan el Consell va decidir restringir la capacitat de difusió dels mitjans estatals russos, com Russia Today o Sputnik, mitjançant la Decisió (PESC) 2022/351, adoptada l'1 de març de 2022, que reforça el règim de sancions davant la campanya sistemàtica de manipulació informativa impulsada pel Kremlin. A més, les persones també poden utilitzar els mecanismes europeus de cooperació penal i judicial per protegir la seua reputació o actuar davant discursos d'odi.

El gran volum d'informació manipulada amb ànim de desprestigiar la UE va portar en 2015 la creació d'una unitat de comunicació estratègica que aglutinara campanyes de contra-desinformació llançades des del Servei d'Acció Exterior (EEAS Stratcom). Va ser una de les primeres accions desenvolupades per la UE en el marc del procés regulador contra la desinformació, arran que el Consell Europeu instara per primera vegada la Comissió Europea a actuar “davant el que consideraven una amenaça creixent per als processos democràtics de la UE i dels seus estats membres” (Colomina i Pérez Soler, 2022, p. 150). La percepció del risc associat a la desinformació en aquell moment estava fortament condicionada tant pel conflicte a Ucraïna i les diferents posicions polítiques dels governs europeus respecte a la Federació Russa.

No va ser suficient i des d'aleshores la UE ha posat en marxa mecanismes legislatius, polítics i judicials que s'emmarquen en una dansa entre l'actuació reactiva, és a dir, destinada a contrarestar la informació falsa o manipulada; i preventiva, que se centra en salvaguardar la llibertat d'informació de la ciutadania en el seu conjunt davant els riscos derivats de la desinformació (Armengol, 2024; Colomina i Pérez Soler, 2022).

Aquest darrer focus és imprescindible perquè, d'acord amb Armengol (2024), les respostes normatives i judicials són “massa lentes i ineficaces” i “en incidir sobre continguts publicats o difosos poden degenerar fàcilment en censura o fins i tot en la creació de discursos oficials o ‘veritats alternatives’ igualment falses” (Armengol, 2024, p. 350). Per tal d'evitar açò es va signar la Declaració conjunta sobre llibertat d'expressió i “notícies falses”, desinformació i propaganda, adoptada a Viena el 3 de març de 2017 per relators internacionals. Entre altres fonaments, estableix que l'acció dels poders públics en matèria de desinformació ha de mantenir-se dins dels límits de la proporcionalitat i de la mínima intervenció necessària i que la protecció ha d'exercir-se en un espai sense fronteres.

El procés regulador de la UE continua amb els Codis de Bones Pràctiques en matèria de desinformació de 2018 i 2022, presentats per la Comissió. Allò que en un primer moment constituïa un mecanisme d'autoregulació sorgit del compromís voluntari entre les institucions europees, els representants de les principals plataformes en línia i de les xarxes socials, així com del sector publicitari, és actualitzat el 2022 preservant l'esquema de corregulació mitjançant un instrument no vinculant. Així, “en comptes d'establir noves normes obligatòries que podrien afavorir una retirada desmesurada de continguts” (Colomina i Pérez Soler, 2022, p. 151), es manté aquest enfocament flexible i s'insisteix en la garantia de la integritat dels serveis, el reforçament dels fact-checkers i l'alfabetització mediàtica dels usuaris, als quals s'encoratja a actuar amb criteri i a informar-se adequadament per identificar la desinformació.

A propòsit d'aquestes mesures sorgeixen dubtes entre els Estats Membres sobre com abordar les qüestions de proporcionalitat i de protecció efectiva de drets fonamentals sense caure en “polèmiques”, és a dir, sobre com moderar continguts a les plataformes digitals sense rebre crítiques que titllen les accions de “censura”. La preocupació principal era:

El doble impacte de la mentida en els sistemes democràtics: d'una banda, pot erosionar la confiança, polaritzar i fins i tot distorsionar el lliure desenvolupament de processos electorals; d'una altra, si l'eliminació d'una mentida nociva s'exerceix de manera desproporcionada i fins i tot arbitrària, el resultat pot impactar en l'exercici de les llibertats individuals i col·lectives (García Morales, 2020, tal com es cita a Colomina i Pérez Soler, 2022, pp. 151-152)

En aquest context, la UE volia anar més enllà del control del contingut i reforçà els límits a la distribució, difusió i capacitat d'influència del contingut maliciós (Colomina i Pérez Soler, 2022). Per això, al desembre de 2018, el SEAE i la Comissió van presentar el Pla d'Acció

contra la Desinformació, que pretenia consolidar la cooperació i el flux d'informació entre aquestes dues institucions i amb els Estats membres a través de la creació d'un Sistema d'Alerta Ràpida (RAS), que s'activa quan es detecten casos de manipulació informativa (Barclay et al., 2023, p. 62).

Més endavant s'aprovà el Pla d'Acció per a la Democràcia Europea de 2020 i es creà l'Observatori Europeu de Mitjans Digitals (EDMO). És més, entre les prioritats de la Comissió en el mandat actual (2024-2029) està lluitar contra la FIMI i les amenaces híbrides, objectiu que s'emmarca en la protecció de la democràcia i per la qual cosa al novembre de 2025 presentà un nou Escut Europeu de la Democràcia per a lluitar contra la manipulació de la informació i les ingerències estrangeres en línia.

3.1 EL PAQUET LEGISLATIU DE SERVEIS DIGITALS I MITJANS

L'evolució significativa a nivell instrumental es va donar, per una banda, amb el desenvolupament de la Divisió East StratCom de l'EEAS (Armengol, 2024; Proto et al., 2025), qui va posar un èmfasi especial en la desinformació digital i els mitjans russos, ja que la nova digitalització de la diplomàcia i l'ús intensiu de les xarxes socials suposaven un repte per als models tradicionals de comunicació diplomàtica. Per afrontar aquesta situació, el SEAE va crear el projecte EUvsDisinfo, que “va ser fonamental per alertar sobre actors estrangers que intentaven aprofitar-se de la pandèmia en benefici propi” (Barclay et al., 2023, p. 62) i actualment té la responsabilitat de desenvolupar pràctiques de *debunking* –desmentir aportant proves– a través d'EUvsDisinfo.

Per altra banda, va ser clau l'aprovació al 2022 del paquet legislatiu de Serveis Digitals, que integra tant la DSA com la DMA. Ambdues adopten la forma de reglament perquè tenen la missió d'armonitzar una normativa cada vegada més dispersa i de cohesionar el mercat únic. La Comissió considerà que estava apareixent “un mosaic de normatives nacionals, com ara les lleis sobre discursos d'odi en línia vigents a Alemanya i França” i buscava evitar una “fragmentació del mercat que dificulta l'entrada de nous actors i consolida la posició dominant de les grans plataformes” a través d'un “marc europeu comú” (Comissió Europea, 2019).

La principal finalitat de la DSA, que és el motor normatiu de la UE en l'àmbit de la resiliència digital i integritat informativa, és promoure la transparència en el mercat digital, aspecte que inclou algorismes i sistemes de recomanació de plataformes tecnològiques (Colomina i Pérez Soler, 2022). Per a la qual cosa, fixa un règim de responsabilitats (arts. 11 a 28 del DSA) perquè els prestadors de serveis col·laboren en la retirada de continguts il·lícits a Internet i estableix obligacions de diligència deguda que son més oneroses depenent del tipus de servicis i de la grandària del prestador (Garrigues, 2024).

Al seu torn, la DMA agrupa diferents lleis dirigides a les grans plataformes digitals que funcionen com *gatekeepers*, amb el propòsit de promoure un model de negoci en l'esfera

online que respecte la privacitat de l'usuari i el dret de la competència. Per això, estan obligades a desenvolupar certes pràctiques i abstindre's de determinades conductes com són les pràctiques monopolístiques (arts. 5, 6 i 7 del DMA).

En l'àmbit de la governança, la DSA i la DMA suposen “la superació del model d'autoregulació aplicat fins el moment” i “el caràcter de ‘poder normatiu’ sobre el qual la UE construeix la seua legitimitat i aportació a l'ordre global” (Colomina i Pérez Soler, 2022, p.154). Tant és el poder que el passat 29 de gener, en el marc de la presentació d'algunes qüestions clau de l'informe de la Comissió Especial sobre l'Escut per a la Democràcia Europea del Parlament Europeu, es va demanar “una aplicació completa de la legislació clau en l'àmbit digital –com ara la DSA, el reglament sobre transparència i segmentació de la publicitat política i la Llei d'Intel·ligència Artificial– a tots els Estats membres” (Parlament Europeu, 2025).

Esta demanda es fa palesa en Estats Membres com Espanya, ja que encara que s'han complert tres anys des que la DSA va entrar en vigor, el Parlament nacional encara no ha desenvolupat les reformes que hi escauen per habilitar legalment a la CNMC com Coordinador de Serveis Digitals tal com demana la norma europea. Tot i que Espanya va ser denunciada per la Comissió Europea davant el TJUE al maig de 2025 per no implementar correctament la llei, junt amb altres països com República Txeca, Xipre, Polònia i Portugal (Agencia EFE, 2025), actualment encara segueix incomplint la DSA.

Com a reacció, més de 20 organitzacions i 40 investigadors es van unir en una carta oberta per a reclamar al Congrés dels Diputats que dote la CNMC de les competències necessàries i així s'aplique la DSA a les grans plataformes i els cercadors. Açò implicaria que assumiren l'obligació d'identificar i reduir els riscos que els seus serveis suposen pels menors d'edat, la salut, les eleccions o la desinformació. Mentrestant, aquesta vulneració del Dret de la UE (DUE) perjudica la recerca i l'accés a les dades, a banda del fet que “els espanyols disfruten de menys garanties i d'una protecció menor que la que tenen altres milions de ciutadans europeus” (Maldita.es, 2025).

No obstant això, el passat 15 d'abril el Ple del Congrés va rebutjar la proposició de llei per habilitar la CNMC com coordinadora de serveis digitals a Espanya i, per tant, no serà tramitada. La moció del Grup Socialista va ser rebutjada amb 174 vots en contra, 163 a favor i 8 abstencions (Congreso de los Diputados, 2026) segons la consulta feta a 28 d'abril de 2026.

3.2 SEGURETAT HUMANA I LLEI DE PREMSA: AI ACT I EMFA

La necessitat de la legislació vista fins ara reforça el fet que el món viu sota una “infocràcia” o “règim de la informació” en el món digital, concepte que Byung-Chul Han (2022) va batejar per explicar “la forma de domini en què la informació i el seu processament mitjançant algoritmes i intel·ligència artificial determinen de mode decisiu els processos

socials, econòmics i polítics” (Traducció pròpia, p. 4). En el marc d’aquesta “infocràcia”, la desinformació i la intel·ligència artificial generativa suposen una amenaça per a la seguretat nacional, donat que el seu ús per a la creació de falsedats impacten en el discurs públic i la seguretat humana, amb grans implicacions per als drets humans i les normes democràtiques (Colomina i Pérez Soler, 2022).

És per això que la IA generativa guarda un lloc especial al dret de la comunicació de la Unió a través d’instruments com la llei d’intel·ligència artificial (AI Act, per les seues sigles en anglés), la DSA o el Reglament Europeu de Llibertat de Mitjans de Comunicació (EMFA, per les seues sigles en anglés). Un exemple de com, segons Serrano Maíllo (2026), en els darrers anys s’ha promulgat un ampli conjunt de disposicions normatives relatives a l’ecosistema europeu orientades, almenys en la seua formulació inicial, a garantir la protecció de la llibertat de premsa i el dret de la ciutadania a accedir a informació veraç i de qualitat.

Es tracta d’una qüestió de plena actualitat. D’una banda, el Tribunal de Justícia de la Unió Europea (TJUE) celebrà el 10 de març de 2026 la seua primera audiència oral dedicada específicament a la relació entre IA generativa i drets d’autor de la premsa en el cas *Like Company v. Google Ireland Limited* (C-250/25). La decisió del TJUE podria fer jurisprudència sobre com s’han d’entrenar i operar els models d’IA dins el mercat europeu i quines obligacions tindran els proveïdors en usar continguts protegits. D’altra banda, els 27 Estats membres de la UE aprovaren el 13 de març una esmena per prohibir els serveis d’IA capaços de generar imatges sexuals falses o despullar persones sense consentiment, en resposta a l’augment de *deepfakes* sexualitzats com la polèmica de Grok, i als riscos que comporten per a la dignitat i la seguretat de les persones.

Durant aquests quatre anys de guerra entre Rússia i Ucraïna, la desinformació també s’ha difós en forma de *deepfakes* de líders polítics i militars, com és el del general Valerii Zaluzhnyi, cap de les forces armades d’Ucraïna, afirmant que el president Zelenski havia ordenat l’assassinat del seu assistent i que Zaluzhnyi es prepararia per a un cop militar contra Zelenski, a qui es referia com “l’enemic del nostre Estat” i culpava com responsable d’un “fracàs complet en la contraofensiva” (StopFake, 2023). Les autoritats ucraïneses i diferents fact-checkers (StopFake, AFP, Full Fact) coincideixen en què es tracta de propaganda russa destinada a fomentar la idea d’un conflicte intern entre l’exèrcit i el govern ucraïnesos.

De fet, la IA generativa crea contingut “independentment de si és facticament correcte o no” (Krack et al., 2026). En aquest procés, pot generar informació errònia o fictícia, incloent-hi fonts inexistents, referències històriques inexactes o fins i tot jurisprudència inventada. Continguts inexactes que són presentats de manera convincent i amb aparença de credibilitat. En aquest sentit, l’última estratègia utilitzada per Rússia inclou la publicació d’informació falsa en Internet i xarxes per tal d’adoctrinar models d’IA com Grok, ChatGPT, Gemini, Perplexity i Copilot.

A sobre, tot i que a Ucraïna no hi ha “una estructura sistemàtica i transnacional de desinformació a escala russa” (Díaz-Merry, 2026, paràgraf 11), el país envaït també ha

utilitzat la desinformació però de manera “menys rellevant i intensiva”, ha assenyalat el professor de la Universidad Autónoma de Madrid especialitzat en seguretat i defensa, Luis de la Corte, en unes declaracions a VerificaRTVE (2026). Per tot açò, la d’Ucraïna es pot considerar “la primera guerra falsejada per la IA”, segons ha afirmat l’expert en tecnologia Jaime García Cantero en una entrevista a la Cadena SER (2026).

La legislació europea esmenta directament els *deepfakes* a normes com el DSA o la Directiva sobre la violència de gènere. A més, l’EMFA menciona el contingut generat per IA. Malgrat que aquestes regulacions de caràcter vinculant estableixen obligacions estrictes per a diversos actors, altres instruments, com les Directrius Electorals de la Comissió Europea i el Codi de Pràctica Reforçat sobre la Desinformació, adopten un enfocament basat en recomanacions i compromisos de naturalesa voluntària per a la gestió de la intel·ligència artificial generativa.

Però la *soft law*, un cop formalitzada, pot tindre efectes jurídics demostrables. Això succeeix amb l’article 45 del DSA, el qual introdueix un model de correulació aplicable als codis de conducta, que s’estén actualment al Codi de Pràctica Reforçat sobre la Desinformació, fet que “en reforça el pes normatiu i la rellevància institucional” (Krack et al. 2026, p. 274). La disposició permet que la Comissió Europea i el Consell articulen compromisos amb plataformes i altres actors rellevants per fer front a riscos sistèmics, inclosa la desinformació:

The Commission and the Board shall encourage and facilitate the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of this Regulation, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks, in accordance with Union law in particular on competition and the protection of personal data (DSA, art. 45).

Adicionalment, la Comissió va adoptar unes directrius sobre pràctiques prohibides d’IA per tal d’aclarir la interpretació de l’article 5 del AI Act, a l’entrada en vigor d’aquestes prohibicions el 2 de febrer de 2025 (Comissió Europea, 2025a). Les directrius informen que, encara que les obligacions de transparència contingudes a l’article 50 tenen com a finalitat reduir l’impacte dels *deepfakes* i dels sistemes de conversa automatitzats, podria haver-hi casos en què, tant si hi ha etiquetes de transparència com si no, s’empren tècniques enganyoses amb efectes rellevants sobre les persones, ja que poden arribar a distorsionar el seu comportament fins al punt que perjudique la seua autonomia i la capacitat de prendre decisions lliures i informades.

Segons Krack et al. (2026), tot i que aquestes directrius no són vinculants, posa a disposició unes eines per interpretar l’AI Act i obrir:

La possibilitat de qualificar determinats sistemes d’intel·ligència artificial utilitzats amb finalitats de desinformació com a pràctiques prohibides, sempre que es complisquen tots els requisits establerts a l’article 5.1.a, és a dir, l’ús de tècniques enganyoses o manipuladores, la distorsió del comportament de les

persones, la producció d'un perjudici significatiu i l'existència d'un nexa causal entre el funcionament del sistema i el dany causat (Traducció pròpia, pp. 277-278)

Davant la possibilitat de la prohibició de certs continguts, les veus expertes demanen tindre en compte un "equilibri" junt amb el dret a la llibertat d'expressió per evitar "conseqüències negatives no desitjades", donada la sensibilitat de la qüestió (Armengol, 2024; Krack et al., 2026).

Aquest debat topa amb l'EMFA, un reglament amb un marc jurídic ferm i garantista que té per objectiu blindar la llibertat editorial, assegurar el major pluralisme dels mitjans de comunicació i garantir la qualitat informativa arreu de la UE. Estableix quatre pilars bàsics sobre els quals s'ha de construir el sistema mediàtic europeu: independència, llibertat, pluralisme i transparència. Després de ser aprovat a l'abril de 2024, el Govern d'Espanya anuncià un conjunt d'actuacions integrades en el seu Pla d'Acció per la Democràcia, destinades a garantir el compliment de les disposicions previstes. Tot i ser una fita dins el marc del DUE de la comunicació, Serrano Maíllo (2026) es pregunta:

Si la millor llei de premsa és aquella que no existeix o, si, per contra, aquest tipus de legislació és necessària en un context com l'actual, en què els atacs a periodistes, els casos de desinformació, la digitalització abusiva, la ingerència estrangera, etc., són cada vegada més freqüents. (Traducció pròpia, p. 294)

És a dir, si el reglament serà la solució a tots aquests desordres informatius o, ben al contrari, serà "un cavall de Troia per a noves maneres de censura" (Maíllo, 2026, p. 297). Una de les raons d'aquesta preocupació rau en el fet que, davant la invasió d'Ucraïna, la UE va bloquejar els canals de difusió russos Russia Today i Sputnik (Consell de la Unió Europea, 2022) i el TJUE en va confirmar la legitimitat (STJUE, 2022). Per això, juristes com Tristante Pellicer i Teruel Lozano (2023) han criticat la severitat d'aquesta mesura argumentant que, fins i tot en temps de guerra, hi ha procediments constitucionals que s'han de respectar:

Aquesta decisió estableix un precedent perillós en atorgar al Consell poders tan amplis, amb tan poques garanties, per restringir una llibertat fonamental: ens trobem davant d'una decisió política, consagrada en un acte jurídic, adoptada sense una base legal clara i sense ni tan sols les garanties més bàsiques, que constitueix una vulneració molt greu d'una llibertat fonamental i minva el pluralisme de l'opinió pública europea (Traducció pròpia, p. 326)

Per altra banda, Kondratov i Johansson-Nogués (2022) sostenen que el caràcter liberal i obert de les societats de França, Alemanya i el Regne Unit han afavorit la ingerència híbrida de Rússia, que atribueixen a l'elevat grau de llibertat d'expressió i a una regulació d'internet relativament laxa. Defensen que aquest escenari ha facilitat que els actors russos orientats a influir en el discurs públic aprofiten l'anonimat i la naturalesa oberta de l'entorn digital, especialment a través de les xarxes socials.

Però tampoc és clar que el bloqueig siga una mesura de pressió eficaç contra Rússia, ja que malgrat que el canal de notícies està actualment bloquejat en els televisors i en l'espai en línia de la UE, EE.UU i Canadà, el mitjà Russia Today continua actiu a Amèrica Llatina. Com que també són hispanohablants, segons un article de Khan (2023) per al Reuters Institute for the Study of Journalism, el Kremlin continua impactant a Espanya a través de canals alternatius de xarxes socials, Telegram i *influencers* locals que afavoreixen la visió russa del conflicte.

Per a les veus expertes entrevistades per Khan (2023), aquests bloquejos poden beneficiar al Kremlin, ja que poden ser entesos com una forma de reconèixer que el Kremlin diu la veritat (la seua postveritat creada) i que les seues tàctiques són efectives; a banda de “no ser útils”, ja que hi ha nombroses maneres d'eludir-los.

Com que tradicionalment la UE ha intervingut per salvaguardar la qualitat del discurs públic i la resiliència democràtica, Pollicino (2026) conclou que “el futur de la llibertat d'expressió en l'era digital es modelarà per aquest delicat equilibri: defensar la veritat sense erosionar el dret a parlar, contrarestar la desinformació sense legitimar noves formes d'arbitrarietat en la moderació de continguts” (p. 530).

3.3 REACCIÓ D'ESPANYA

A Espanya no hi ha una llei de premsa específica contra la desinformació. La legislació espanyola contra la desinformació es fonamenta en un marc legal divers: la normativa europea, una actualització de la legislació nacional del Dret de Rectificació (que es troba en fase de tramitació parlamentària) i l'Ordre PCM/1030/2020, que estableix un procediment d'actuació coordinat pel Consell de Seguretat Nacional per detectar i respondre a campanyes de desinformació que busquen desestabilitzar institucions o processos electorals. Amb la possible actualització de la norma que regula el Dret a la Rectificació es podrà demanar, en un màxim de 20 dies i de manera immediata, la correcció d'afirmacions falses difoses per mitjans de comunicació digitals i influencers de xarxes socials.

L'actual marc inclou la Comissió Permanent de Lluita contra la Desinformació (eina de coordinació institucional entre els diferents òrgans de l'Administració) i es complementa amb mecanismes per a la protecció de menors i la lluita contra *deepfakes*, així com amb l'aplicació del Codi Penal per a casos de difusió vinculats amb delictes d'odi, revelació de secrets, contra la integritat moral o contra la salut pública, entre d'altres.

L'Ordre, que es basa en el Pla d'Acció contra la Desinformació de 2018 presentat pel SEAE i la Comissió, estableix quatre nivells d'alerta que, al seu torn, estructuren la resposta davant campanyes de desinformació que puguen posar en perill la seguretat nacional. Mentre que el nivell 1 dona capacitat per actuar a nivell tècnic en la seua monitorització i vigilància, incloent la participació en el Sistema d'Alerta Ràpida de la UE (RAS) i la seua notificació, el nivell 2 ja eleva el seu seguiment i avaluació a la Comissió Permanent contra la Desinformació per tal que es definisquen propostes d'actuació i s'active, si escau, una

cèl·lula de Coordinació contra la desinformació per part del Director del Departament de Seguretat Nacional.

El nivell 3 s'activa quan una alerta de desinformació adquireix una rellevància elevada i requereix una gestió coordinada a escala política-estratègica, però encara sense atribució formal a un Estat tercer. Finalment, el nivell 4 representa el grau màxim d'alerta i s'activa quan existeix una atribució pública d'una campanya de desinformació a un Estat tercer, cosa que transforma la situació en una qüestió de seguretat nacional i política exterior. En aquest escenari, el Consell de Seguretat Nacional assumeix la coordinació de la resposta política, donada la gravetat de l'amenaça i les seues possibles implicacions internacionals.

En conjunt, per tal de lluitar contra la desinformació, a Espanya es distribueixen responsabilitats entre actors de naturalesa diversa, incloent-hi, d'una banda, el Govern central i, de l'altra, la resta d'organismes públics amb competències en aquest àmbit, així com el sector privat i la societat civil (Badillo i Arteaga, 2024). Per tant, diversos governs autonòmics tenen competències en matèria de seguretat, mentre que la defensa és responsabilitat de l'administració central; i totes disposen de competències directes en qüestions de comunicació social (art. 148-149 CE).

A aquests grups s'afegeix un nou actor dins l'ecosistema informacional: els fact-checkers, que són organitzacions que naixen com una resposta de caràcter autorregulador impulsada tant per la recerca acadèmica com pels mitjans de comunicació. Es va començar a manifestar a inicis del segle XXI a EE.UU amb [FactCheck.org](https://factcheck.org) o Politifact. Les primeres experiències a Espanya inclouen Miniver.org. al 2017, Newtral i [Maldita.es](https://maldita.es) al 2018 o EFEVerifica i Verificat al 2019 (López Pan i Rodríguez Rodríguez, 2019).

L'informe d'IBERIFIER (Badillo i Arteaga, 2024) assenyala que, tot i que encara són limitades, és previsible que en el futur les comunitats autònomes incrementen la seua implicació en la detecció i la lluita contra la desinformació dins l'àmbit de les seues competències, especialment vinculada a les polítiques de comunicació i sensibilització social.

En aquest context, algunes comunitats han començat a desenvolupar iniciatives específiques. Catalunya constitueix un cas rellevant perquè l'any 2021 la Generalitat va impulsar un projecte orientat a combatre la desinformació relacionada amb la migració de joves d'origen marroquí, mentre que el Consell Audiovisual de Catalunya (CAC), en col·laboració amb el Departament d'Educació, ha desenvolupat el programa eduCAC, centrat en l'alfabetització mediàtica i digital, amb una atenció específica a la identificació de notícies falses. Altres territoris, com el País Basc, han incorporat la problemàtica de la desinformació dins de programes formatius en matèria de ciberseguretat, mentre que en altres comunitats aquestes polítiques es troben encara en una fase incipient o poc desenvolupada (Badillo i Arteaga, 2024).

A escala estatal, cal destacar la creació d'una ponència específica de Seguretat Nacional en el si de la Comissió Mixta Congrés-Senat, que analitza el fenomen de la desinformació de

manera continuada des de l'any 2021. Aquesta es deu a l'Estratègia de Seguretat Nacional del mateix any, que va incloure per primer cop les campanyes de desinformació com una amenaça per a la seguretat nacional i identificà la necessitat d'esforços públic-privats per abordar-les. El fòrum està compost per sis representants de l'administració pública i deu de la societat civil, el periodisme, l'acadèmia i la indústria de la comunicació (Departamento de Seguridad Nacional, 2023, p. 4).

En aquest marc, el fòrum contra les campanyes de desinformació en l'àmbit de la seguretat nacional elabora treballs en què tracta mesures existents per a identificar les pràctiques desinformatives, com respondre i en quins casos, recomanacions de bones pràctiques, així com consensuar mecanismes més eficients per fer-los front des del respecte als drets i llibertats fonamentals consagrats en la Constitució.

Per altra banda, com a país membre de l'OTAN, Espanya col·labora amb l'Aliança, ens que preveu un mecanisme de doble via per contrarestar la desinformació a través de la comprensió de l'entorn informatiu i la prevenció de l'efectivitat de les amenaces. Primer supervisa periòdicament aquest tipus d'informacions i després desenvolupa una comunicació proactiva, que inclou explicacions i proves sobre l'estat de l'espai informatiu, per tal que l'audiència pugui entendre, confiar i creure en la seua tasca. Usualment l'OTAN exposa la desinformació d'actors estrangers a través del seu portal web *Setting the Record Straight*.

Atès que l'Aliança concep la desinformació com un fenomen de naturalesa genuïnament global, Braže (2022) assenyala que l'OTAN considera la coordinació amb els aliats i socis com un element central de la seua actuació. En coherència amb aquest focus, col·labora amb les nacions aliades i sòcies i altres actors internacionals com el SEAE, la Comissió Europea, el Centre de Compromís Global del Departament d'Estat dels Estats Units, el Mecanisme de Resposta Ràpida del G7 i les Nacions Unides.

4. REGULACIONS A NIVELL GLOBAL I VISIÓ SOTA DRET INTERNACIONAL

A aquesta secció es fa una anàlisi dels instruments jurídics que s'han utilitzat a nivell global per fer front a la desinformació, així com a nivell nacional en alguns Estats Membres de la UE. S'ha de tindre en compte que, com s'ha mencionat anteriorment, la desinformació és un fenomen que afecta tots els països d'arreu del món i que s'estén principalment a l'esfera digital.

L'estudi de 2023 de Lim i Bradshaw va trobar que entre 2011 i 2022 s'adoptaren 105 lleis per combatre la desinformació, la manipulació i la *malinformation* en 78 països a escala global. Tot i que algunes d'aquestes normes tenen com a objectiu reforçar la transparència de les plataformes digitals i promoure l'alfabetització mediàtica, moltes altres criminalitzen la producció i la difusió de les anomenades "notícies falses" (Ginsborg, 2026).

La causa d'aquesta criminalització a l'àmbit legislatiu es troba en la manca d'una definició internacional de la desinformació en matèria jurídica. Són regulacions freqüentment utilitzades per atacar l'oposició política, amb algunes definicions que vinculen directament la difusió d'informació falsa amb actes terroristes, com passa, per exemple, a Egipte, l'Aràbia Saudita i la Federació Russa, i poden vulnerar el dret a expressar opinions.

Segons Ginsborg (2026), la manca d'atenció adequada al principi de seguretat jurídica permet extreure lliçons valuoses de l'àmbit de la lluita antiterrorista. L'absència d'una definició internacional clara de terrorisme va crear un escenari propici perquè alguns règims legitimaren polítiques repressives contra l'oposició política. És per això que l'expert proposa una analogia amb el cas de la desinformació, donat que la crisi de la Covid-19 va impulsar l'aprovació massiva de noves normes en aquesta matèria, malgrat que des de feia anys tant alguns responsables polítics com la societat civil advertien dels riscos que aquestes mesures podien comportar per als estàndards de drets humans i els principis fonamentals de la democràcia mateixa.

En aquest sentit, les lleis o esborranys del Regne Unit, l'Índia, Austràlia, Brasil, Bangladesh, França, Singapur i Tanzània foren objecte de preocupació per a l'Oficina de l'Alt Comissionat de l'ONU per als Drets Humans (UN OHCHR, 2021), qui observà que contenien definicions deficientes sobre què constitueix "contingut il·legal" o "nociu" i per tant eren perilloses per a la llibertat d'expressió (Ginsborg, 2026, p. 75).

La llibertat d'expressió està protegida pel dret internacional, així com pel dret de la UE i pel dret nacional. L'article 19 de la Declaració Universal dels Drets Humans estableix que "tothom té dret a la llibertat de pensament i d'expressió; aquest dret inclou la llibertat de mantenir opinions sense interferència i de cercar, rebre i difondre informació i idees per qualsevol mitjà i sense límits fronterers". D'acord amb la sentència del Tribunal Europeu de Drets Humans (TEDH) en *Handyside contra el Regne Unit* (1976), aquesta llibertat d'expressió no es limita a les "declaracions correctes", sinó que també protegeix "informació i idees que ofenen, pertorben o incomoden l'Estat o una part de la població, ja que així ho exigeixen el pluralisme, la tolerància i l'esperit d'obertura propis d'una societat democràtica" (paràgraf 49).

Per tant, en el cas de la prohibició d'informació, el dret a la llibertat d'expressió únicament es pot limitar si es fonamenta en criteris i circumstàncies específiques tal com estableix l'article 19.3 del Pacte Internacional de Drets Civils i Polítics (PIDCP). Segons aquesta disposició, els Estats poden introduir limitacions sempre que aquestes superen un control tripartit. En primer lloc, qualsevol restricció ha d'estar establerta per una norma amb rang de llei, formulada amb un grau suficient de claredat i precisió perquè les persones puguin anticipar-ne les conseqüències. En segon lloc, la mesura ha de respondre a una finalitat legítima, restringida als supòsits que s'enumeren en el propi article: la salvaguarda dels drets o la reputació dels altres, la protecció de la seguretat nacional o de l'ordre públic, així com la defensa de la salut o la moral públiques. Finalment, la ingerència ha de resultar necessària i proporcional en relació amb l'objectiu perseguit. En aquest sentit, Stasi i Parcu (2021, p. 412) insisteixen en

què les garanties consagrades a l'article 19 del PIDCP exigeixen una anàlisi rigorosa i una delimitació precisa del concepte de desinformació que es pretén sancionar.

4.1 LLEIS INTERNES EN ELS ESTATS MEMBRES

En el cas de França, el seu Parlament, al 2018, va aprovar una [lleï contra “la manipulació de la informació”](#), comunament anomenada la “lleï de la desinformació” o “lleï de les *fake news*”, la qual segueix en vigor segons la consulta feta a 4 de maig de 2026. La legislació té l'objectiu de frenar la difusió d'informació falsa durant les campanyes electorals, obligant les plataformes digitals a mecanismes de transparència.

A les disposicions s'estableix un nou procediment civil destinat a aturar la desinformació durant els tres mesos anteriors als comicis. Així, es permet que els partits polítics apelen un jutge per tal que avalue, en un termini de 48 hores, si una informació falsa es difon de manera “artificial o automàtica” i “a gran escala” d'acord amb l'art. L163-2 del *Code électoral*. La multa consisteix en un any de presó i 75.000 euros a aquell que difonga aquest tipus de contingut segons l'art. L112 del *Code électoral*.

Així mateix, atribueixen al Consell Superior Audiovisual francès el poder “d'impedir, suspendre o interrompre la difusió de serveis de televisió controlats per un estat estranger o sota la influència d'aquest estat i que puguin minar la integritat de les eleccions” (Traducció pròpia, Llei orgànica n° 2018-1202 del 22 de desembre de 2018, art. 6).

La llei va ser criticada per organitzacions com Reporters Sense Fronteres o el Sindicat Nacional de Periodistes de França, qui consideraven “ambigua” la seua definició d’“informació falsa” (Perelló, 2024) i que, per tant, obria les portes a abusos o interpretacions desafortunades per part dels tribunals. A més, el Rapporteur de Nacions Unides (UN OHCHR, 2021) i l'acadèmia (Stasi i Parcu, 2021) alertaren de la privatització de la justícia en atribuir a les plataformes digitals el deure de discernir entre què és *fake news* i què no ho és, sumat al fet que el curt termini per retirar continguts, junt a les fortes multes, podia empènyer les plataformes a eliminar continguts que no són clarament odiosos només per evitar sancions.

Per la seua banda, Alemanya va adoptar la seua [Llei de Control de les Xarxes](#) al 2017, una legislació que, segons Stasi i Parcu (2021), és actualment una de les “més estrictes” en matèria de moderació de continguts. Aquesta obliga a les plataformes de xarxes socials de més de dos milions d'usuaris al seu territori que eliminen el discurs d'odi, la difamació i les incitacions a la violència, així com els símbols nazis i la negació de l'Holocaust. De forma similar a la norma francesa, inclou una definició imprecisa o incompleta sobre “continguts manifestament il·lícits” i elevades sancions econòmiques que propicien pràctiques de control excessiu.

Per altra banda, a Itàlia, la resposta a la desinformació combina iniciatives reguladores i mecanismes policials, però amb “resultats limitats” (Stasi i Parcu, 2021). El panell tècnic creat per l'*Autorità Garante per le Comunicazioni* (Autoritat Garant de la Comunicació o AGCOM) el 2017, de caràcter voluntari, ha tingut un impacte reduït, tot i que ha aportat una anàlisi rellevant mitjançant [informes recents](#). Paral·lelament, des de 2018 existeix un sistema de denúncia de notícies falses gestionat per la policia, que ha estat criticat, com s’ha vist anteriorment, per la manca d’una definició clara sobre “continguts manifestament il·lícits”, ja que utilitza criteris com “el possible impacte sobre l’ordre públic”.

En aquest context, tot i que el terme “desinformació” pot resultar operatiu com a categoria analítica en l’àmbit de la recerca acadèmica i com a eina orientadora en el disseny de polítiques públiques, la seua translació a l’àmbit jurídic planteja reptes significatius. Cal dotar-lo d’una definició més precisa i clara, que garantisca la seguretat jurídica tant de la ciutadania com dels operadors privats de contingut en línia. Ja siga consensuada a nivell internacional o estatal, ha de servir no sols per orientar l’actuació d’aquests operadors, sinó també per protegir eficaçment els drets fonamentals, evitar abusos regulatoris i preservar els principis bàsics de l’estat de dret en l’entorn digital.

4.2 INTERVENCIONISME PER GARANTIR LLIBERTATS I OPINIÓ PÚBLICA

En aquest punt resulta inevitable fer referència a la importància que té l’estat de dret per a la dimensió normativa de la llibertat d’expressió i preguntar-se si l’actuació dels Estats en aquesta matèria és una intervenció legítima. Seguint el debat clàssic propi de la filosofia política, depèn de si entenem aquesta llibertat com un dret natural i inherent a l’ésser humà, com sostenia Locke (John, 2019), o com un dret polític que pren sentit dins d’una comunitat política organitzada (Habermas, 1989).

D’acord amb la teoria de l’acció comunicativa i la democràcia deliberativa de Habermas, qui defensava una “racionalitat comunicativa” (1984, pp. 8–20), l’intervencionisme estatal en la regulació de la llibertat d’expressió és necessari per tal de protegir l’espai públic i mantindre’l com un lloc de diàleg lliure de coaccions. És a dir, l’Estat ha d’intervindre amb l’objectiu legítim de garantir que els ciutadans puguin participar amb igualtat de condicions en la formació de l’opinió pública i la voluntat política a través del diàleg racional, entenent la llibertat d’expressió com una eina de sobirania popular.

Amb l’expansió d’Internet, Habermas sosté que la intervenció estatal esdevé encara més necessària per evitar que els algoritmes condicionen l’opinió pública i per salvaguardar la integritat del procés deliberatiu davant informacions manipulades. En aquest marc, com una resposta reguladora a la crisi de l’esfera pública en l’era de les plataformes, la UE ha decidit combatre la desinformació amb tres grans pilars: la regulació de les plataformes digitals, la protecció de la independència dels mitjans de comunicació i la transparència en la publicitat política.

Mitjançant l'aprovació de normatives com la DSA, la DMA, l'EMFA, el Reglament sobre publicitat política i l'AI Act, la UE ha impulsat un gir innovador i rellevant en la governança de l'espai informatiu digital. Aquest conjunt d'iniciatives suposa una ruptura amb el model d'autoregulació que havia prevalgut fins ara, tal com es reflectia en la legislació nacional dels Estats membres. Tot i que el paquet de mesures s'aplica al mercat únic de la UE, aquest ha contribuït a l'anomenat "efecte Brussel·les", aplicant-se sovint com estàndard global i aconseguint un impacte extraterritorial que persegueix, finalment, tindre conseqüències directes sobre el poder de les grans tecnològiques (Colomina i Pérez Soler, 2022) i ser un actor important en la regulació de l'espai digital.

5. CONCLUSIÓ

Després de l'anàlisi realitzada, es pot concloure que la UE assumeix que la defensa de l'espai digital, el pluralisme mediàtic i el bon funcionament del debat públic requereixen una intervenció pública activa i no poden quedar en mans exclusivament del mercat o de l'amenaça d'actors externs. Una concepció que, si comparem amb altres països, difereix radicalment de la postura dels Estats Units, marcada pel pes central de la Primera Esmena. La interpretació expansiva de la llibertat d'expressió ha convertit qualsevol intent de regulació pública de la desinformació en un terreny pràcticament inaccessible, fins i tot quan la circulació de continguts falsos o enganyosos té efectes demostrables sobre el funcionament dels mecanismes democràtics (Pollicino, 2026) i la seguretat nacional.

Una seguretat nacional que, si bé a l'era actual es considera un bé públic fonamental que l'Estat ha de garantir, a la UE hi domina el debat central sobre com s'ha d'equilibrar amb el dret a la informació i a la llibertat d'expressió amb la intenció de fer front a la desinformació sense assumir un paper censor. La raó principal és que l'estratègia europea s'ha concentrat durant anys en la regulació d'allò que es publica, mentre que només en una fase més recent ha començat a abordar el problema de com es difon la informació. En aquest nou gir, iniciatives impulsades pel SEAE en el marc de la FIMI busquen actuar sobre els mecanismes de propagació, més que no pas sobre els continguts en si.

Pel que fa al marc de la FIMI, tal com s'està aplicant des de la UE, tendeix a quedar restringit a la identificació d'operacions d'influència atribuïdes principalment a Rússia i la Xina, cosa que en limita l'abast analític i polític. Aquesta focalització contrasta amb la trajectòria recent de Rússia, marcada per un ús intensiu i adaptable de la guerra informativa com a eina central per configurar les percepcions sobre la seua invasió a gran escala d'Ucraïna, tant a nivell intern com internacional. L'exclusió dels canals informatius europeus va obligar Moscou a reconfigurar els seus mecanismes d'influència mitjançant vies alternatives, com actors marginals, nous perfils d'influència i pràctiques d'intel·ligència tradicionals, alhora que desplaçava el seu focus cap a les audiències del Sud Global. En aquest context, els canvis polítics de finals de 2024, com l'elecció de Donald Trump, evidencien les mancances del concepte FIMI a l'hora d'afrontar possibles intents d'incidència sobre l'opinió pública europea per part d'altres actors internacionals, com els Estats Units o Israel, i posen de relleu

fins a quin punt la guerra informativa forma part estructural de l'estratègia geopolítica russa davant els seus rivals occidentals.

Tot i que la UE ha assenyalat Rússia i la Xina com a principals rivals en l'àmbit narratiu, aquesta delimitació podria acabar tenint efectes contraproductius sobre l'eficàcia de la seua diplomàcia pública. En la mesura que el marc FIMI podria aplicar-se a qualsevol actor internacional que intente influir en les preferències dels actors polítics europeus, existeix el risc que aquestes iniciatives siguin percebudes com a mesures de contenció o sanció, generant respostes defensives per part dels actors afectats. Tal com adverteix Valenza (2021, p. 4) a l'anàlisi de Proto et al. (2025), aquest enfocament comunicatiu resulta problemàtic perquè passa per alt que els intercanvis entre societats només poden ser realment fructífers quan l'acció exterior incorpora de manera plena els principis de reciprocitat i mutualitat.

Les estratègies de resposta davant la manipulació i la ingerència informativa estrangera continuen obertes i lluny d'estar plenament definides. En aquest escenari incert, el SEAE ha estat l'actor capaç de reaccionar amb més agilitat, especialment si es compara amb altres institucions europees i amb els parlaments dels Estats membres, sovint condicionats per entorns polítics interns fragmentats i altament polaritzats. A aquesta complexitat s'hi afegeix la naturalesa mateixa de la infodèmia, caracteritzada per la sobreabundància de continguts i la volatilitat de les narratives, que dificulten identificar quins discursos tenen una capacitat real d'influència i justifiquen una intervenció prioritària.

Com que està previst que la FIMI russa s'intensifiqui durant el 2026, el pressupost per a l'ingerència informativa estrangera s'ha augmentat un 7 % respecte a l'any anterior, fins arribar als 1,56 mil milions d'euros (SEAE, 2026). Aquest fet mostra com la desinformació també està afectant la monetarització i la revisió financera tant en els pressupostos públics com en les organitzacions privades. Així mateix, s'espera que les regions del mar Bàltic i de l'Àrtic figuren entre els principals objectius en l'àmbit informatiu i és altament probable que Rússia perpetue narratives sobre l'ordre mundial multipolar que desacrediten la UE i la idea d'Occident. Per tant, davant la necessitat constant d'augment de recursos, la resposta no ha de provindre únicament de l'àmbit de la comunicació o l'acció exterior, sinó que ha d'involucrar a persones de lideratge i de diferents equips o sectors, és a dir, que s'hauria d'incrementar l'abast del SEAE.

Davant d'aquest context, una ampliació del paper de la UE en el bloqueig directe d'informació, com va posar de manifest el caràcter excepcional de la prohibició de RT i Sputnik, podria acabar debilitant els seus principals avantatges normatius i comportar més pèrdues que beneficis. En lloc d'això, caldria desplegar un ventall renovat d'eines que permetés abordar el fenomen amb més flexibilitat, com amb la dotació de més veu o poders als fact-checkers i l'Observatori Europeu de Mitjans Digitals. A això s'afegeix que la Unió només ha anat incorporant de manera gradual la lògica del control informatiu en la seua acció exterior, mentre que, simultàniament, se li exigeix mantenir una coherència estricta amb un enfocament normatiu basat en regles en la gestió de la desinformació dins del mercat interior.

Per últim, convindria ampliar la investigació per tal de determinar els efectes de la FIMI russa a cada Estat membre a través d'enquestes, participació electoral i entrevistes a fact-checkers nacionals, així com amb l'estudi dels algoritmes a Internet i xarxes per tal de frenar determinats continguts artificiosos. La identificació de correlacions espúries poden afectar les conclusions generals dels mecanismes digitals. En definitiva, un engranatge de desestabilització en processos electorals a nivell mundial al qual cal dedicar més esforços.

BIBLIOGRAFIA

ARMENGOL FERRER, F. (2024). Desinformación en la Unión Europea: de la guerra híbrida al espacio europeo de la libertad de información. A M. I. Serrano Maíllo & L. Corredoira y Alfonso. (Eds.), *Democracia y desinformación: nuevas formas de polarización, discursos de odio y campañas en redes. Respuestas regulatorias de Europa y América Latina* (pp. 345–362). Dykinson. <https://dialnet.unirioja.es/servlet/articulo?codigo=9637167>

BARCLAY, M., PERGER, I., & SALVAI, M. (2023). Fighting the fallacies: The “infodemic” and the European Commission. A T. D. Purnat, T. Nguyen, & S. Briand (Eds.), *Managing infodemics in the 21st century: Addressing new public health challenges in the information ecosystem* (pp. 53–71). Springer Nature. <https://doi.org/10.1007/978-3-031-27789-4>

BRAŽE, B. (2022). La OTAN y la nueva agenda de desinformación de Rusia. El futuro de la OTAN tras la cumbre de Madrid 2022. *Cuadernos de Estrategia*, 211. Instituto Español de Estudios Estratégicos. Ministerio de Defensa. <https://isbnsearch.org/isbn/9788490916438>

CASTELLS, M. (1996). *The Rise of the network society*. Blackwell.

CASTELLS, M. (2008). Los medios y la política. *Telos: Revista de Pensamiento, Sociedad y Tecnología*, 74, 1–14. <https://telos.fundaciontelefonica.com/archivo/numero074/los-medios-y-la-politica/>

CASTELLS, M. (2009). *Comunicación y poder*. Alianza Editorial.

COLOMINA, C., & PÉREZ-SOLER, S. (2022). Desorden informativo en la UE: construyendo una respuesta normativa. *Revista CIDOB d'Afers Internacionals*, 131, 141–146. <https://doi.org/10.24241/rcai.2022.131.2.141>

DOV BACHMANN, S. D., PUTTER, D., & DUCZYNSKI, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*, 14(5), 858–869. <https://doi.org/10.1111/1758-5899.13257>

GINSBORG, L. (2026). International human rights law and the legal regulation of disinformation. A L. GINSBORG & P. GORI (Eds.), *Disinformation*, (pp. 71–93). Springer.

HABERMAS, J. (1984). *The Theory of Communicative Action. Volume 1: Reason and the rationalization of society*. Beacon Press.

HABERMAS, J. (1989). *The structural transformation of the public sphere: Inquiry into a category of bourgeois society*. MIT Press.
<https://teddykw2.wordpress.com/wp-content/uploads/2012/07/jurgen-habermas-theory-of-communicative-action-volume-1.pdf>

HOFFMAN, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
https://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf

JOHN, R. R. (2019). Freedom of expression in the digital age: A historian's perspective. *Church, Communication and Culture*, 4(1), 25–38.
<https://doi.org/10.1080/23753234.2019.1565918>

KONDRATOV, E., & JOHANSSON-NOGUÉS, E. (2023). Russia's Hybrid Interference Campaigns in France, Germany and the UK: A Challenge against Trust in Liberal Democracies? *Geopolitics*, 28(5), 2169–2199.
<https://doi.org/10.1080/14650045.2022.2129012>

KRACK, N., DUTKIEWICZ, L., & DE MEYERE, J. (2026). Generative artificial intelligence and disinformation. A L. GINSBORG & P. GORI (Eds.), *Disinformation*, (pp. 259–291). Springer. https://doi.org/10.1007/978-3-032-00480-2_15

LEITE, J. A., RAZUVAYEVSKAYA, O., BONTCHEVA, K., & SCARTON, C. (2024). EUvsDisinfo: A dataset for multilingual detection of pro-Kremlin disinformation in news articles. *Proceedings of the 33rd ACM International Conference on Information and Knowledge Management*, 5380–5384. Association for Computing Machinery.
<https://doi.org/10.1145/3627673.3679167>

LÓPEZ PAN, F., & RODRÍGUEZ RODRÍGUEZ, J. M. (2019). El fact checking en España: Plataformas, prácticas y rasgos distintivos. *Estudios sobre el Mensaje Periodístico*, 26(3), 1045-1065. Ediciones Complutense. <https://doi.org/10.5209/esmp.65246>

OKHOLM, C. S. (2026). The Russo-Ukrainian Information War. A GINSBORG, L., GORI, P. (Eds.), *Disinformation*, (pp. 355-376). Springer, Cham. https://doi.org/10.1007/978-3-032-00480-2_19

PADALKO, H. (2025). AI and information manipulation: Russia's interference in the US elections. *Digital Policy Hub Working Paper*, Centre for International Governance Innovation. <https://www.cigionline.org/publications/ai-and-information-manipulation-russias-interference-in-the-us-elections/>

POLLICINO, O. (2026). Freedom of Expression and Its Limits: Constitutional Dilemmas and Regulatory Conundrum Related to the Fight Against Disinformation. A GINSBORG, L., GORI, P. (Eds.), *Disinformation*, (pp. 513-532). https://doi.org/10.1007/978-3-032-00480-2_26

PROTO, L., LAMOSO-GONZÁLEZ, P., & GARCÍA, L. B. (2025). The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight. *Media and Communication (Lisboa)*, 13(S4). <https://doi.org/10.17645/mac.9474>

ROUDAKOVA, N. (2017). *Losing Pravda: Ethics and the press in post-truth Russia*. Cambridge University Press. <https://doi.org/10.1017/9781316817117>

SERRANO MAÍLLO, M. I. (2026). El Reglamento Europeo de Libertad de Medios (EMFA) como instrumento de protección de las libertades informativas. *Revista Española de la Transparencia*, (23, Extra 2026). <https://doi.org/10.51915/ret.445>

STASI, M. L., & PARCU, P. L. (2021). Disinformation and misinformation: The EU response. A P. L. PARCU & E. BROGI (Eds.), *Research handbook on EU media law and policy*, (pp. 407–426). Edward Elgar Publishing. <https://doi.org/10.4337/9781786439338.00030>

TRISTANTE PELLICER, L., & TERUEL LOZANO, G. M. (2023). Desinformación y libertad de expresión: el bloqueo europeo de canales rusos ante la invasión de Ucrania a la luz de la Sentencia del Tribunal General (Gran Sala) de 27 de julio de 2022, T-125/22, RT France c. Consejo de la UE. *Estudios de Deusto*, 71(2), 303–329. <https://doi.org/10.18543/ed.2936>

TORRALBA, F., GARCÍA DEL MURO, J., & RUIZ, C. M. (2020). *Veritat, postveritat i fake news*. Pagès Editors.

WEBGRAFIA

AGENCIA EFE. (2025, 7 de maig). *Bruselas lleva a España al TJUE por la ley de servicios digitales*. <https://efe.com/euro-efe/2025-05-07/bruselas-espana-tjue-ley-europea-servicios-digitales/>

CADENA SER. (2026, 28 de març). *La primera guerra falseada por inteligencia artificial: de los deepfakes a las armas autónomas en Ucrania*. <https://cadenaser.com/nacional/2026/03/28/la-primera-guerra-falseada-por-inteligencia-artificial-de-los-deepfakes-a-las-armas-autonomas-en-ucrania-cadena-ser/>

CONGRESO DE LOS DIPUTADOS. (2026, 15 d'abril). *El Pleno rechaza dos proposiciones de ley sobre uso del velo integral y para habilitar a la CNMC como coordinadora de servicios digitales* [Nota de prensa]. https://www.congreso.es/es/notas-de-prensa?p_p_id=notasprensa¬asprensa_notaid=51272

DÍAZ-MERRY, B. (2026, 24 de febrer). *Guerra de Ucrania: cuatro años de desinformación y bulos*. RTVE Verifica. <https://www.rtve.es/noticias/20260224/desinformacion-bulos-deepfakes-cuatro-anos-guerra-ucrania/16950520.shtml>

EUVSDISINFO. (2025, 23 d'octubre). *Grandes modelos de lenguaje: un nuevo frente en la guerra informativa rusa*.
<https://euvsdinfo.eu/es/grandes-modelos-de-lenguaje-un-nuevo-frente-en-la-guerra-informativa-rusa/>

GARRIGUES. (2024, 14 de febrer). *El Reglamento de Servicios Digitales (DSA) en 46 preguntas*.
https://www.garrigues.com/es_ES/garrigues-digital/reglamento-servicios-digitales-dsa-46-preguntas

KAHN, G. (2023, 30 de març). *Bloqueada en Occidente, la propaganda rusa prospera en español en TV y redes sociales*. Reuters Institute for the Study of Journalism.
<https://reutersinstitute.politics.ox.ac.uk/es/news/bloqueada-en-occidente-la-propaganda-rusa-prospera-en-espanol-en-tv-y-redes-sociales>

KLECZKOWSKA, A. (2025). *The Russian Disinformation Campaign During the Romanian Presidential Elections: A Violation of International Law?* Opinio Juris.
<https://opiniojuris.org/2025/01/27/the-russian-disinformation-campaign-during-the-romanian-presidential-elections-the-perfect-example-of-a-violation-of-international-law/>

MALDITA.ES. (2024, 6 de novembre). *Desmentiment sobre la comitiva del Rei i pàgines russes i àrabs*. <https://maldita.es/malditobulo/20241106/comitiva-rey-paginas-rusas-arabe/>

MALDITA.ES. (2025, 30 de maig). *Investigación sobre Pravda News en español en España*.
<https://maldita.es/investigaciones/20250530/pravda-news-espanol-espana/>

MALDITA.ES. (2025, 17 de juliol). *Análisis de 300 contenidos de Pravda sobre el atentado de Torre Pacheco*.
<https://maldita.es/investigaciones/20250717/300-contenidos-pravda-torre-pacheco/>

MALDITA.ES. (2025, 16 de novembre). *Carta DSA*. Congreso de los Diputados.
<https://files.maldita.es/maldita/uploads/2025/11/69170a8abf071.pdf>

PERELLÓ, B. (2024, 1 de maig). *Desde Francia hasta Turquía: así se ha legislado contra los bulos y la desinformación en otros países.* Newtral. <https://www.newtral.es/legislacion-desinformacion/20240501/>

RTVE. (2025, 22 maig). *Seguridad Nacional atribuye a Rusia campañas de desinformación sobre la DANA para promover desconfianza ciudadana.* <https://www.rtve.es/noticias/20250522/seguridad-nacional-atribuye-rusia-campanas-desinformacion-dana-promover-desconfianza-ciudadana/16592188.shtml>

STOPFAKE. (2023, 8 de noviembre). *Fake: Ukrainian Commander-in-Chief Zaluzhny Is Preparing a Military Coup.* <https://www.stopfake.org/en/fake-ukrainian-commander-in-chief-zaluzhny-is-preparing-a-military-coup/>

UN OHCHR. (2021). *Moderating online content: fighting harm or silencing dissent?* <https://www.ohchr.org/en/stories/2021/07/moderating-online-content-fighting-harm-or-silencing-dissent>

VERIFICA EFE. (2025). *El apagón en España y Portugal y la campaña prorrusa de desinformación.* <https://verifica.efe.com/apagon-espana-portugal-campana-prorrusa-desinformacion/>

WALLNER, C., COPELAND, S., & GIUSTOZZI, A. (2025). *Russia, AI and the future of disinformation warfare.* Royal United Services Institute. <https://www.rusi.org/explore-our-research/publications/emerging-insights/russia-ai-and-future-disinformation-warfare>

INFORMES I DOCUMENTS INSTITUCIONALS

AGÈNCIA DE LA UNIÓ EUROPEA PER A LA CIBERSEGURETAT I SERVEI EUROPEU D'ACCIÓ EXTERIOR. (2022, desembre). *Foreign information manipulation interference (FIMI) and cybersecurity—Threat landscape*. European Union Agency for Cybersecurity (ENISA).
<https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape>

BADILLO, Á., & ARTEAGA, F. (2024, abril). *El impacto estratégico de la desinformación en España*. IBERIFIER / Real Instituto Elcano.
<https://media.realinstitutoelcano.org/wp-content/uploads/2024/04/informe-iberifier-el-impacto-estrategico-de-la-desinformacion-en-espana.pdf>

COMISSIÓ EUROPEA. (2019, agost). DGx proposed priorities paper [Document de treball intern]. Directorates-General of the European Commission.
https://www.politico.eu/wp-content/uploads/2019/08/clean_definite2.pdf

SERVEI EUROPEU D'ACCIÓ EXTERIOR. (2025, gener). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the architecture of FIMI operations*. EEAS.
https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

SERVEI EUROPEU D'ACCIÓ EXTERIOR. (2026, març). *4th EEAS annual report on foreign information manipulation and interference threats*. EEAS.
https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf

PARLAMENT EUROPEU. (2025, 18 de desembre). *Draft report on the findings and recommendations of the Special Committee on the European Democracy Shield*. PE 775.431. Special Committee on the European Democracy Shield. https://www.europarl.europa.eu/doceo/document/EUDS-PR-775431_EN.pdf

DEPARTAMENTO DE SEGURIDAD NACIONAL. (2023, desembre). *Foro contra las campañas de desinformación en el ámbito de la seguridad nacional: Trabajos 2023*. Presidencia del Gobierno de España. <https://www.dsn.gob.es/sites/default/files/documents/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf>

WARDLE, C., & DERAKHSHAN, H. (2017, octubre). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Report DGI-09. Directorate General of Human Rights and the Rule of Law of the Council of Europe. <https://firstdraftnews.org/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-de-CC%81sinformation-1.pdf>

NORMATIVA

CONSELL DE LA UNIÓ EUROPEA. (2022). Decisió (PESC) 2022/351 del Consell, d'1 de març de 2022, per la qual es modifica la Decisió 2014/512/PESC relativa a mesures restrictives motivades per les accions de Rússia que desestabilitzen la situació a Ucraïna. DOUE, L 65, pp. 5–7. <https://eur-lex.europa.eu/eli/dec/2022/351/oj>

LOI ORGANIQUE N° 2018-1201, du 22 décembre 2018, relative à la lutte contre la manipulation de l'information [Llei orgànica n.º 2018-1201, de 22 de desembre de 2018, relativa a la lluita contra la manipulació de la informació]. Journal Officiel de la République Française n.º 0297, 23.12.2018. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847556>

ORDRE PCM/1030/2020, de 30 d'octubre, per la qual es publica el Procediment d'actuació contra la desinformació aprovada pel Consell de Seguretat Nacional. BOE núm. 292, 05.11.2020, pp. 96673–96680. <https://www.boe.es/eli/es/o/2020/10/30/pcm1030>

REGLAMENT (UE) 2022/2065 DEL PARLAMENT EUROPEU I DEL CONSELL, de 19 d'octubre de 2022, relatiu a un mercat únic de serveis digitals. DOUE L 277, 27.10.2022, pp. 1–102. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R2065>

REGLAMENT (UE) 2022/1925 DEL PARLAMENT EUROPEU I DEL CONSELL, de 14 de setembre de 2022, sobre mercats disputables i equitatius en el sector digital. DOUE L 265, 12.10.2022, pp. 1–66. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R1925>

JURISPRUDÈNCIA

TRIBUNAL EUROPEU DE DRETS HUMANS. (1976). Assumpte 5493/72 *Handyside contra el Regne Unit*, de 7 de desembre de 1976, § 49. <https://hudoc.echr.coe.int/eng?i=001-57499>

TRIBUNAL GENERAL DE LA UNIÓ EUROPEA. (2022). Assumpte C 340/55 RT *France contra Consell de la Unió Europea* de 27 de juliol de 2022. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62022TA0125>

DECLARACIÓ RESPONSABLE SOBRE ÚS DE LA IA

Reconec l'ús d'eines d' IA durant el procés d'elaboració d'aquesta recerca, sempre amb la meua posterior revisió i edició, de tal manera que **cap contingut generat per tecnologies d'IA ha sigut presentat com el meu propi treball**. La responsabilitat de l'autoria i del contingut final recau exclusivament en la signant de l'article.

A continuació, faig un desgranament de les eines utilitzades, explicant-ne el seu objectiu i abast, per tal de rendir comptes i ser transparent, mostrar quins beneficis pot aportar l'algoritme i assumir que és responsabilitat, tant de l'acadèmic com del periodista, conèixer, investigar la IA i cercar la millor forma de treballar amb ella. Perquè mentre es faça un ús responsable, pot ser una aliada de l'ofici.

Recerca preliminar de bibliografia

Eina utilitzada: Gemini

Propòsit: Es va usar per a la recerca preliminar de bibliografia i noms d'autors o autores o institucions investigadores sobre les quals desenvolupar una posterior investigació (amb paraules clau) a bases de dades obertes com Web of Science, Scopus o la biblioteca de la UAB.

Prompts o instruccions proporcionades: Es donà una descripció detallada sobre l'objectiu del treball (defensa de l'opinió pública davant la desinformació d'agents estrangers, especialment provinent de Rússia) i que es buscava tant institucions com investigadors acadèmics i experts en aquesta qüestió, a poder ser una llista d'autories igualitària (evitar visió masculinitzada).

Ús del contingut generat: S'acceptaren alguns suggeriments.

Revisió i edició: Tots els suggeriments foren revisats manualment. Posteriorment s'amplià amb recerques i lectures pròpies a unes altres bases de dades.

Limitacions i consideracions ètiques: No es va utilitzar automàticament sense revisió. Només eren alguns noms per començar la recerca.

Justificació de l'elecció: Gemini destaca per la seua integració profunda amb internet i per tant té més informació actualitzada

Revisió d'introducció de cites i correcció de format de citació

Eina utilitzada: Claude

Propòsit: Es va usar per a la millora de la redacció a l'hora d'introduir cites literals al text (de més de 40 paraules) i per a corregir el format APA7 de les cites.

Prompts o instruccions proporcionades: Es preguntà quines eres maneres idònies de donar pas a una cita acadèmica literal llarga o quins exemples reals a texts acadèmics em podia donar. Per al format de citació, es facilità l'exemple oficial de la pàgina APA7 perquè fera correccions pertinents.

Ús del contingut generat: S'acceptaren correccions d'APA7, mentre que les frases d'introducció de cites foren reformulades.

Revisió i edició: Tots els suggeriments foren revisats per mantindre coherència conceptual i gramatical (adequació d'acord amb les normes en el cas de citació).

Limitacions i consideracions ètiques: No es va utilitzar l'eina per a l'anàlisi o desenvolupament de la investigació juridicopolítica ni redacció de cap de les parts d'aquest treball. S'ha sigut curosa per tal d'evitar plagi. La responsabilitat de l'autoria i del contingut final recau exclusivament en la signant del treball.

Justificació de l'elecció: Claude ajusta el text a la guia d'estil de la redacció personal i és l'eina preferida per periodistes que busquen una escriptura més ètica

Explicació sobre com netejar una taula d'Excel

Eina utilitzada: ChatGPT

Propòsit: Es va usar per a demanar instruccions sobre com realitzar algunes tasques en la neteja d'una taula Excel. Amb aquestes explicacions, es va poder continuar endavant per aconseguir una taula dinàmica amb la qual elaborar un mapa a Datawrapper.

Prompts o instruccions proporcionades: Es preguntà quins passos s'havien de seguir per dividir algunes caselles d'una base de dades que havia descarregat a Mendeley i EUvsDisinfo per tal de dividir la desinformació per països i poder fer un recompte.

Ús del contingut generat: S'acceptaren instruccions.

Revisió i edició: Es va poder treballar amb Excel i seguir editant la taula d'acord amb els paràmetres del periodisme de dades.

Limitacions i consideracions ètiques: No es va utilitzar l'eina per crear un gràfic des de zero. Només es demanà ajuda per tal d'aconseguir netejar una base de dades molt extensa. El gràfic (en aquest cas un mapa) va ser elaborat per la signant.

Justificació de l'elecció: ChatGPT és útil per proporcionar guies pas a pas i explicar conceptes.

Recerca de verificació d'un *deepfake*

Eina utilitzada: Google Fact Check Explorer

Propòsit: Es va usar per a cercar si el deepfake sobre l'ambaixador d'Ucraïna al Regne Unit, Valerii Zaluzhnyi, com el pròxim president d'Ucraïna havia sigut desmentit professionalment i quins mitjans de la International Fact-Checking Network ho havien fet.

Prompts o instruccions proporcionades: Es va cercar amb paraules clau com el cognom i “Ucraïna”.

Ús del contingut generat: S'acceptaren els resultats.

Revisió i edició: Es va llegir el contingut dels desmentits i es va reformular per explicar aquest cas.

Limitacions i consideracions ètiques: No es va utilitzar l'eina per copiar les explicacions sobre la verificació, sinó com eina per corroborar la falsedat de la desinformació.

Justificació de l'elecció: Google Fact Check Explorer és un cercador que indexa les verificacions professionals realitzades pels membres de la IFCN. Permet realitzar recerques per text o imatge en diferents idiomes. És una bona font d'informació verificada.