EDICIONES COMPLUTENSE

Derecom
e-ISSN: 1988-2629

ARTÍCULOS

Análisis FIMI de la desinformación en las elecciones españolas de 2023: objetivos, canales y narrativas para dañar la confianza en el sistema electoral

Rodrigo Cetina-Presuel
UPF Barcelona School of Management (España)

Catalina Gaete-Salgado
Universidad Complutense de Madrid (España)

https://dx.doi.org/10.5209/dere.99490 Recibido: 05/12/2024 • Revisado: 11/01/2025 • Aceptado: 26/02/2025

ES **Resumen.** Los procesos electorales contemporáneos se desarrollan en un ecosistema informativo altamente digitalizado, protagonizado por plataformas de redes sociales y herramientas algorítmicas que han terminado con la intermediación editorial de los medios de comunicación. En un escenario donde la regulación aún es emergente, y donde las instituciones se adaptan progresivamente a la transformación tecnológica, el sistema electoral es vulnerable a la desinformación inundando el debate público. Con el objetivo de recabar evidencia de los desórdenes informativos en contexto electoral, el Observatorio Complutense de Desinformación desarrolló una metodología a partir de la taxonomía FIMI (*Foreign Information Manipulation and Interference*) del Servicio Exterior de la Unión Europea, y la aplicó en misiones de observación electoral en 14 países. Este estudio presenta los resultados de ese proceso en las elecciones españolas de 2023, donde se identificó el objetivo de deslegitimar ciertos aspectos del proceso electoral, utilizando a Whatsapp como principal canal de distribución. Las reacciones y medidas ante bulos electorales fueron contundentes desde la sociedad civil, pero mejorables desde las plataformas de redes sociales y las instituciones del Estado. En la discusión se analiza lo observado, y se finaliza ofreciendo recomendaciones para mejorar la capacidad de respuesta de todos los actores del sistema democrático, que, ante una amenaza polifacética como la desinformación, deben actuar en colaboración.
Palabras clave. Desinformación, Desórdenes Informativos, Procesos electorales, FIMI, Instituciones democráticas.

ENG FIMI analysis of disinformation in the 2023 Spanish elections: objectives, channels and narratives to damage confidence in the electoral system

ENG **Abstract.** Contemporary electoral processes take place in a completely digitized information ecosystem, through social media platforms and algorithmic tools that have put an end to the editorial intermediation of legacy media. In a scenario where regulation is still emergent, and where institutions are progressively adapting to technological transformation, the electoral system is highly vulnerable to manipulative narratives and disinformation flooding the public debate. In order to gather evidence of information disorders in an electoral context, the Observatorio Complutense de Desinformación developed a methodology, adapted from the European External Action Service's FIMI taxonomy, and applied it in election observation missions in 14 countries. This particular study shows the results of that observation in the Spanish elections of 2023, where the goal of delegitimizing certain aspects of the electoral process was identified, using Whatsapp as the main distribution channel. The reactions and measures against electoral hoaxes were strong from civil society, but response from social media platforms and state institutions should be improved. In the discussion, this paper first analyzes what was observed, to then offer recommendations to improve the response capacity of all the actors of the democratic system, who, in the face of a multifaceted threat such as disinformation, must act in collaboration.
Keywords. disinformation, information disorders, electoral processes, FIMI, democratic institutions.

Sumario. 1. Introducción. 1.1. Descripción del escenario político-electoral de España en 2023. 2. Marco teórico. 2.1. Preocupación por el fenómeno. 2.2. El combate a la desinformación. 2.3. En busca de un esquema para analizar interferencias. 3. Metodología. 3.1 Conformación de la muestra. 3.2. Metodología de análisis y codificación. 4. Análisis y resultados. 4.1 Objetivos de la desinformación. 4.2 Medios de distribución de la desinformación. 4.3 Autores causantes de la desinformación. 4.4. Destinatarios de la desinformación. 4.5.

Narrativas y metanarrativas de desinformación. 4.6. Reacciones y medidas adoptadas. 5. Discusión. 5.1 Sobre el contenido desinformador y sus objetivos. 5.2. Sobre los medios de distribución de la desinformación. 5.3. Sobre las reacciones y medidas. 6. Conclusiones. 7. Referencias.

Cómo citar: Cetina-Presuel, R. y Gaete-Salgado, C. (2025). Análisis FIMI de la desinformación en las elecciones españolas de 2023: objetivos, canales y narrativas para dañar la confianza en el sistema electoral. *Derecom* 38(1), 29-44. https://dx.doi.org/10.5209/dere.99490

1. Introducción

Las elecciones contemporáneas se desarrollan en un ecosistema informativo de alto riesgo. Rubio-Núñez et al (2024) indican que las campañas electorales premodernas, que se valían principalmente de estrategias de propaganda individual, a partir del contacto personal entre candidatos y electores, mutaron a la intermediación de los grandes medios de comunicación de masas, como la radio y la televisión en el siglo XX. Sin embargo, en el siglo XXI, el escenario es radicalmente diferente.

En las campañas electorales actuales, los entornos públicos están altamente digitalizados, permitiendo una forma de contacto más dinámica e interactiva. Esto permite a partidos y candidatos imponer sus propias agendas informativas, lo que desconfigura la intermediación editorial de los medios de comunicación y su monopolio en la formación de una opinión pública libre (González-Urbaneja, 2023; Bustos-Gisbert, 2021). Sin filtro periodístico, y con redes sociales internamente diseñadas en torno a un modelo de negocio basado en la captura de la atención y no en la información fiable (Jungherr & Schroeder, 2021), las narrativas conspirativas, los mensajes de odio y la desinformación se han vuelto prominentes en el espacio público. En un escenario electoral, estas narrativas y teorías conspirativas –muchas veces promovidas por fuentes anónimas o sintéticas– distorsionan el debate político, tan consustancial al proceso, "creando amenazas concretas al pacto social y al funcionamiento regular de las instituciones que lo garantizan" (Rubio-Núñez et al, 2024, p.47).

Con el propósito de aportar evidencia sobre este fenómeno, en el marco de procesos electorales reales, el Observatorio Complutense de Desinformación se abocó a la tarea de monitorizar casos de desinformación, narrativas hostiles e interferencias informativas en diferentes procesos electorales[1]. Hasta noviembre de 2024, el Observatorio ha llevado a cabo 14 misiones de observación electoral[2], donde ha desarrollado, aplicado y refinado el método de análisis FIMI (*Foreign Information Manipulation and Interference*) del Servicio Exterior de la Unión Europea adaptándolo para la observación de desinformación alentada por actores nacionales, y no solo internacionales. El principal objetivo de esta observación es la identificación de los elementos constitutivos de la desinformación electoral y sus posibles antídotos, que permitan la posterior comparación entre países, la identificación de buenas prácticas y la confección de sugerencias y recomendaciones para actores relevantes, como órganos electorales y organismos regulatorios.

Una de estas misiones de observación fue la de las elecciones españolas de 2023, donde se trabajó en conjunto con el medio verificador Maldita.es para la identificación de bulos electorales y posterior carga en una plataforma equipada con herramientas de inteligencia artificial para identificar narrativas y metanarrativas. La observación electoral se llevó a cabo gracias al trabajo de 10 estudiantes del máster universitario en Políticas Públicas y Sociales de la Barcelona School of Management de la Universidad Pompeu Fabra (UPF-BSM), coordinados por un equipo de investigadores del Observatorio Complutense de Desinformación.

Este artículo condensa la presentación del análisis de 124 casos de desinformación electoral identificados en las elecciones españolas de 2023, incluyendo las autonómicas y municipales de mayo y las generales de julio.

1.1. Descripción del escenario político-electoral de España en 2023

Superado el escollo sanitario, económico y social de la pandemia del COVID-19, el año 2023 comenzaba con las elecciones autonómicas y municipales convocadas para el 28 de mayo en doce comunidades autónomas, siguiendo lo dispuesto por la legislación electoral en el caso de las municipales, y los estatutos en el caso de las autonómicas. Ese día, el mapa político español cambió completamente.

Los resultados de las elecciones autonómicas y municipales del 28 de mayo dieron por ganador al partido de Alberto Núñez Feijóo, el Partido Popular

1 Este trabajo se desarrolló en el marco de dos proyectos: Proyecto "Garantías frente a la desinformación en procesos electorales", centrado en ciberseguridad y desórdenes informativos. Proyecto Next Generation: "La ciberseguridad en los procesos electorales. Garantías frente a la desinformación y otros desórdenes informativos en plataformas" (CYBERELECTIONS) Referencia TED2021-130876B-I00, financiado por el Ministerio de Ciencia e Innovación, y el proyecto "Garantías institucionales y regulatorias. autoridades electorales y de supervisión digital ante interferencias, narrativas hostiles, publicidad segmentada y polarización" (Dir-Politics), Referencia PID2022-137245OB-I00, financiado por el Ministerio de Ciencia e Innovación y la Agencia Estatal de Investigación.

2. Hasta noviembre de 2024, los países en donde se ha llevado a cabo la observación electoral son Colombia, Guatemala, República Dominicana, Panamá, Venezuela, Argentina, Chile, Brasil, México, Uruguay, España, Estados Unidos, Ecuador y Costa Rica.

(PP). El PP ganó las municipales por tres puntos porcentuales y más de dos mil concejales. En las autonómicas, el PP también logró superar al principal partido de gobierno, el Partido Socialista Obrero Español (PSOE), en el número de presidencias, ganando por mayoría absoluta en tres comunidades, más Ceuta y Melilla; y conformando gobiernos de coalición en las demás. En tanto, el PSOE sólo logró conservar tres presidencias autonómicas.

Ante la derrota de su partido, Pedro Sánchez, líder del PSOE y presidente del gobierno de coalición, tomó la inesperada decisión de adelantar las elecciones generales para el 23 de julio, y lo anunció al día siguiente de la celebración de los comicios municipales y autonómicos. Con su decisión, la izquierda se reorganizó. La vicepresidenta primera, Yolanda Díaz, configuró una nueva coalición política, la plataforma Sumar, con la que "absorbe" al partido que, hasta entonces, formaba parte de la coalición de gobierno, Podemos. Así, figuras insignes del partido a la izquierda del PSOE, como la entonces vicepresidenta Irene Montero, quedan fuera de las listas[3].

En el marco de una convocatoria electoral para el mes de julio, la campaña se desarrolló en periodo estival, con las juntas electorales abocadas a echar a andar el sistema con una mayor proporción de votos por correo y un número mayor de excusas para conformar las mesas (López-Nieto, 2024). Simultáneamente, se negociaban los acuerdos para la presidencia de comunidades autónomas y municipalidades, en donde el PP necesitó del partido a su derecha, VOX, para formar gobierno en varios ayuntamientos y comunidades. Este fue el caso de la Comunidad Valenciana, Aragón, Murcia y Baleares. Este escenario de negociaciones marcó la campaña electoral de julio de 2023, configurando un escenario de alta polarización política[4].

La descripción del contexto político-electoral ya vislumbra algunos de los elementos esenciales del sistema que fueron explotados para la confección de contenido desinformador y que serán presentados en la sección de resultados: la prominencia del voto por correo debido al periodo estival fue una de las dianas preferidas por las principales narrativas desinformadoras que circularon durante el periodo analizado, denunciando reiteradamente la comisión de supuesto fraude electoral con base en dicha modalidad de votación. Esto implicó un ataque directo a la Junta Electoral Central (JEC) y las juntas provinciales y de zona, los órganos de la administración electoral a cargo de garantizar la integridad del proceso. Además, entre los resultados más relevantes del estudio destaca que un 27% de los bulos no tuvo ninguna reacción o medida durante el periodo analizado. Es decir que casi un tercio de los casos de desinformación electoral no tuvo aclaración o verificación de alguna autoridad electoral, como sí se ha visto en otras experiencias de observación como, por ejemplo, en las elecciones de Estados Unidos (Corredoira & Gaete, 2024). Tampoco contaron con la verificación de un *fact-checker* o con la reacción de las plataformas, que como se ha visto también en otros procesos, pueden eliminar o limitar el contenido desinformador.

Estos resultados contribuyen a describir el escenario de la desinformación en España a partir de datos y evidencia recolectada en un proceso electoral real. Con ello, sirve también como un insumo para la formulación de respuestas y reacciones de los organismos del Estado, y como un modelo metodológico replicable en futuros procesos.

2. Marco teórico

2.1. Preocupación por el fenómeno

Desde la Unión Europea se ha alertado sobre la amenaza particular que la desinformación representa para los procesos electorales, momento clave en que los ciudadanos deben contar con información fiable sobre su derecho a voto, la fecha y lugar de la elección, la seguridad de los sistemas de votación y los métodos válidos para emitir el voto (Comisión Europea, 2018). Además, se ha puesto de relieve que los ciudadanos también necesitan información veraz sobre los candidatos y sus preferencias de política pública; por lo tanto, las campañas políticas son esenciales para asegurar un espacio equitativo para presentar y comunicar sus programas y políticas (Fletcher et al, 2018). Al mismo tiempo, la complejidad de los procesos electorales y las leyes que los regulan los hacen particularmente vulnerables a la desinformación, lo que dificulta a los ciudadanos navegar por un sistema complejo, reduciendo su capacidad de separar la realidad de la información engañosa.

El fenómeno de la injerencia electoral puede definirse como un conjunto de formas ilegítimas e injustificadas de influenciar a las personas y su elección de voto, de tal manera que su habilidad para ejercer derechos políticos se vea reducida (Sivalo, 2024). Las campañas de desinformación electoral buscan engañar a los votantes de manera intencionada (Judge & Korhani, 2020) y para ello utilizan información falsa distribuida a sabiendas. Los desinformadores también se valen del uso de identidades falsas, de difundir descontextualizaciones, contenido verdadero pero presentado de manera engañosa y que lleva a conclusiones equivocadas, amplificando la división social y la desconfianza. Estas estrategias buscan que el ciudadano también pierda la confian-

3 Para saber más sobre la negociación que dio forma a la plataforma Sumar, y su impacto en Podemos, ver el artículo titulado "Podemos pierde el pulso con Díaz y queda diluido en Sumar: del 'dedo' de Iglesias al veto a Montero", escrito por María Menéndez para el portal web de RTVE y publicado el 10 de junio de 2023. Disponible en el siguiente enlace: https://www.rtve.es/noticias/20230610/sumar-podemos-acuerdo-coalicion-elecciones-23j/2449072.shtml

4. Sobre el escenario de polarización, ver los siguientes artículos periodísticos:
"PP y Vox buscan el cambio el 23J y la izquierda remontar los sondeos en otra campaña polarizada" (9 de julio de 2023), Agencia EFE. Disponible en el siguiente enlace: https://efe.com/espana/2023-07-09/polarizacion-confrontacion-campana-23j/
"Un 2023 de alto voltaje político llega a su fin: 'superaño' electoral con la amnistía como protagonista" (26 de diciembre de 2023), RTVE. Disponible en el siguiente enlace: https://www.rtve.es/noticias/20231226/resumen-politico-ano-2023-alto-voltaje-amnistia/2467930.shtml

za en las fuentes de información fiable (McKay & Tenove, 2021).

Para inundar la esfera pública con información engañosa y crear incertidumbre en la ciudadanía (Krafft & Donovan, 2020), los desinformadores se valen, sobre todo, de las tecnologías digitales, en particular de las redes sociales (Fernández, 2024), algo que autores como Wardle & Derakhshan (2017), en el plano internacional, o Corredoira y Alfonso (2023) en el español, han llamado *desórdenes informativos.*

La investigación en torno a los desórdenes informativos ha centrado uno de sus múltiples esfuerzos en desentrañar el impacto concreto de los bulos, encontrando serias dificultades para establecer una relación causal entre la exposición a la información falsa y un cambio en las actitudes o comportamientos de las personas (Schünemann, 2022). Esto es particularmente relevante en un contexto electoral donde no se puede probar que la desinformación cambie la intención de voto, sino más bien que la información falsa tiende a reforzar percepciones y decisiones preexistentes (Syrovátka, Hořejš & Komasová, 2023). Sin embargo, sigue siendo objeto de preocupación el impacto de la desinformación a largo plazo (Schünemann, 2022), por cómo los desórdenes informativos en su conjunto dejan un rastro de desconfianza en las instituciones democráticas y en su habilidad para reflejar la voluntad de los ciudadanos (Sivalo, 2024; McKay & Tenove, 2021). Por ello, es necesario que los países democráticos tengan sistemas adecuados de respuesta a estos fenómenos.

2.2. El combate a la desinformación

La desinformación es un problema polifacético. Sin duda, los propios ciudadanos contribuyen a los desórdenes informativos que afectan a nuestra sociedad, y los algoritmos de las plataformas de internet juegan también un papel al priorizar el contenido que más atención genera (European Court of Auditors, 2021), sin importar su calidad. En este sentido, debe resaltarse que, en tanto dichos algoritmos estén vinculados a un modelo de negocio enfocado en la captura de la atención y no en la distribución de información fiable y veraz, son particularmente vulnerables a la manipulación por actores maliciosos (Jungherr & Schroeder, 2021). Muchas de las herramientas que son parte integral del ecosistema digital de hoy, como la recopilación y análisis de datos personales, la publicidad digital y otras herramientas, pueden ser cooptadas por aquellos que se dedican a desinformar (European Commission, 2018). Por otro lado, el uso documentado de la Inteligencia Artificial (IA) en campañas electorales revela cómo la tecnología puede ser utilizada para socavar procesos democráticos, con estrategias de manipulación de la realidad, tales como *deepfakes* y *astroturfing*, entre otros (Rubio-Núñez et al, 2024).

A todo ello no ayuda que las plataformas digitales, a pesar de su considerable poder e influencia en la manera en que nos comunicamos y la información que consumimos a través de sus algoritmos, insistan en verse a sí mismas como meros canales que vehiculan la expresión de terceros (Starr, 2020) negando tener cualquier responsabilidad editorial o sobre la calidad de la información que en sus entornos se disemina (Cetina-Presuel & Martínez-Sierra, 2019), posiblemente porque esto les ha ayudado a evadir los esfuerzos por regularlas (Gillespie, 2018), algo para lo que el nuevo Reglamento de Servicios Digitales europeo (DSA)[5] es una contribución necesaria pero aún de resultados inciertos (Cetina-Presuel 2024a; Cetina-Presuel 2024b).

A la desinformación también contribuyen actores políticos, medios de comunicación y otros actores de la sociedad civil que se aprovechan de las oportunidades que internet nos ha dado para comunicarnos y compartir información a gran velocidad, pero que también ha vuelto a nuestro ecosistema informativo más vulnerable a las injerencias y la manipulación (Marwick & Lewis, 2017). En este escenario, es esencial prestar especial atención a los esfuerzos sistemáticos y coordinados de interferir en los procesos por medio de la desinformación, particularmente aquellos esponsorizados por gobiernos que buscan obstaculizar los procesos democráticos en beneficio propio y que a menudo utilizan herramientas híbridas que aún no se entienden plenamente (Iosifidis & Nicoli, 2020).

Como se ha dicho, la desinformación no tiene una sola causa atribuible y, por lo tanto, no existe una sola vía para solucionarlo (Comisión Europea, 2018). Las intervenciones respecto a la circulación de información engañosa o inexacta no solo pueden interferir con usos legítimos de las tecnologías digitales, también pueden chocar frontalmente con la libertad de expresión, con el discurso político e interponerse en la participación política de los votantes informados (Judge & Korhani, 2020).

Al ser un problema polifacético, también requerirá de diversas soluciones cuya efectividad sólo puede determinarse de manera adecuada con un estudio preciso del fenómeno. Por ello, las respuestas que se den han de estar basadas en evidencia y en un conocimiento lo más pleno posible del ecosistema informativo y la desinformación que circula en el mismo, así como de los actores que buscan difundirla para distorsionar el proceso y la opinión pública para ganancia propia, los destinatarios (candidatos, entes electorales o partes del proceso electoral) a los que atacan y los medios que utilizan para ello.

2.3. En busca de un esquema para analizar interferencias

Uno de los focos de la lucha contra la desinformación digital se ha puesto en los actores extranjeros que buscan utilizarla para interferir en otras democracias (Schünemann, 2022). Cuando se trata de estos actores, parece evidente que se busca desestabilizar a las instituciones democráticas y por lo tanto a los sistemas políticos de naciones rivales

5 REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). Disponible en español en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R2065

para alcanzar metas políticas o económicas (Bennett & Livingston, 2018). De ahí que las taxonomías desarrolladas para el análisis de la manipulación de información e interferencia (*Foreign Information Manipulation and Interference,* o FIMI por sus siglas en inglés) desarrolladas por, entre otros, el Servicio Europeo de Acción Exterior[6] y la OTAN[7] sean particularmente útiles.

Como se verá con mayor detalle en la metodología, las FIMI pueden definirse como aquellos patrones de comportamiento que pueden impactar negativamente en los procesos políticos de un país objetivo, aún si se trata de actividades que no son ilegales, pero sí manipulativas, y llevadas a cabo de manera coordinada e intencional por actores estatales y por terceros (Yuskiv & Karpchuk, 2024). Estas taxonomías son útiles para identificar, describir y entender acciones coordinadas por actores estatales extranjeros, como el caso de Rusia, cuyas acciones han sido ampliamente documentadas (European Court of Auditors, 2021).

Sin embargo, hoy se sabe que la desinformación, sea esponsorizada por un Estado o sea obra de terceros, no proviene exclusivamente del extranjero ni es una actividad que esté reservada solamente a regímenes autoritarios o a dictadores (Iosifidis, 2024). También se trata de actividades que provienen y se coordinan desde dentro. La desinformación se ha infiltrado en las democracias.

Ejemplos como los vividos en Estados Unidos y Reino Unido en 2016, y más claramente en 2020, o en Brasil, donde los líderes de sus respectivos gobiernos han alentado la desinformación, cuando no directamente coordinado campañas desinformadoras, son evidencia de que también los actores políticos locales se valen de la manipulación y la interferencia para avanzar sus esfuerzos de consolidar el poder, aún si es a costa de sus propias instituciones democráticas. En consonancia con las narrativas identificadas por FIMI a nivel exterior, las narrativas internas a menudo presentan a las instituciones electorales como un enemigo que habilita el fraude, narrativa que se refuerza cuando el resultado de la elección es contrario a las pretensiones de uno u otro grupo.

De ahí que, así como las metodologías FIMI han sido refinadas para describir la sofisticación de los esfuerzos de desinformación extranjeros, sea necesario adaptarlas para lograr identificar, describir y descifrar los esfuerzos domésticos de desinformación, sea esta más o menos coordinada. Por ello, desde el Observatorio Complutense de Desinformación se propone una adaptación de las FIMI, enfocando la metodología para identificar, clasificar y entender la manipulación de la información e interferencia, pero centrándose en los fenómenos locales. Con esta metodología se busca "medir las principales características de la desinformación en período electoral con parámetros estandarizados y replicables", adaptando las "taxonomías validadas por la comunidad de ciberseguridad, a contextos electorales nacionales en tiempos de paz"[8]. Para ello, se han extendido las categorías originales de FIMI, para lograr entender mejor los actores, incidentes, objetivos y técnicas que aparecen en un contexto de desinformación electoral.

Una de las principales diferencias es que la FIMI es particularmente útil para identificar actores extranjeros y entender cómo operan, intentando con ello determinar lo más precisamente posible el origen (extranjero) de la desinformación para intentar ponerle freno. En cambio, la metodología desarrollada por el Observatorio se centra en entender el fenómeno desinformativo local de manera más descriptiva, centrándose en los impactos negativos de la desinformación, lo que ha permitido ampliar las categorías de autores causantes de desinformación previstas en las taxonomías FIMI para introducir a actores relevantes en los contextos nacionales como los pseudomedios, a los llamados *influencers,* a aquellos que amplifican –aunque no originan– la desinformación, además de candidatos, entes gubernamentales locales y partidos políticos.

Así, la metodología presentada en este estudio está adaptada para entender los impactos de la desinformación en procesos electorales, catalogar y describir las reacciones y medidas adoptadas frente a incidentes de desinformación (desde comunicados de instituciones públicas a recursos en sede judicial, a verificación de noticias por parte de *fact-checkers*, y sus correspondientes desmentidos pasando por medidas tomadas por las propias plataformas de redes sociales como la retirada de contenidos o su etiquetado como información no fiable). Los resultados y conclusiones de este trabajo permiten hacer recomendaciones basadas en evidencia para reforzar ciertas respuestas a la desinformación o introducir otras nuevas, más efectivas.

La metodología adaptada de FIMI ayuda a identificar si existe o no una cierta acción coordinada y permite hasta cierto punto identificar el origen de las narrativas, pero se centra primordialmente en identificar al autor causante, o bien al que amplifica un incidente de desinformación, su destinatario y los objetivos que se persiguen al desinformar sobre el mismo. Además, cataloga los canales utilizados para distribuir desinformación y las técnicas utilizadas (como la manipulación, la fabricación de contenidos, el uso de *bots* o perfiles falsos, información sacada de contexto, etc.).

Así, en el ámbito nacional o local, FIMI ayuda a entender cómo ciertas narrativas, y ciertos actores desinformadores, que actúan o bien como originadores de la desinformación o como amplificadores de la misma, llegan a poner en peligro el desarrollo normal de una elección. Esto puede ser porque se

6 Para más información sobre la estrategia del Servicio de Acción Exterior de la Unión Europea, ver el artículo en su web, titulado: Tackling Disinformation, Foreign Information Manipulation & Interference (actualizado al 14 de noviembre de 2024), disponible en el siguiente enlace: https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

7 Para más información sobre la estrategia de la Organización del Tratado del Atlántico Norte (OTAN), ver el artículo en su web, titulado: NATO's approach to countering disinformation (actualizado al 8 de noviembre de 2023), disponible en el siguiente enlace: https://www.nato.int/cps/en/natohq/topics_219728.htm

8. Metodología del Observatorio Complutense de Desinformación explicada en su sitio web y disponible en el siguiente enlace: https://www.ucm.es/observatoriodesinformacion/observacion_electoral

mina la confianza en el proceso, se desalienta la participación, se alienta la polarización o se intenta destruir la reputación del rival político o incluso del propio órgano electoral garante de la contienda. Todo esto ha permitido desarrollar un libro de códigos que se ha puesto a disposición de aquellos que se dedican a investigar sobre la desinformación, sus causas y sus efectos[9].

3. Metodología

3.1. Conformación de la muestra

La muestra analizada en el marco de las elecciones españolas de 2023 provino de una alianza con el medio verificador Maldita.es, una organización sin ánimo de lucro constituida en 2019 bajo la figura de fundación.

Maldita.es recibe casos de desinformación, principalmente, a través de un *chatbot* de WhatsApp[10], en donde los usuarios pueden enviar bulos circulantes en sus propias plataformas de redes sociales y pedir al medio que lo verifique. Además, el equipo periodístico monitorea regularmente las redes sociales, desde donde también pueden identificar bulos. Según explica el propio medio en un apartado metodológico disponible en su página web[11], los criterios para seleccionar los casos que se verificarán siguen los criterios de viralidad (alcance en redes sociales) y peligrosidad (contexto de aparición del bulo, situación de crisis). En el mismo apartado metodológico destacan que "(n)o todo es verificable: sólo comprobamos los datos y hechos que son susceptibles de ser contrastados. No verificamos opiniones, aunque sí señalamos las falsedades que las sustentan en su caso". Agregan que, independientemente de la persona o institución objeto de la desinformación, los criterios metodológicos aplicables son los mismos.

Para abarcar los dos hitos electorales ocurridos en 2023 –las elecciones autonómicas y municipales del 28 de mayo y las generales del 23 de julio– se determinó un periodo de recolección de datos entre el 19 de mayo y el 17 de octubre de 2023. De esta manera, se han podido abarcar casos de desinformación ocurridos antes, durante y después de los comicios. En el periodo indicado, el *chatbot* de WhatsApp de Maldita.es recibió 22.257 contenidos provenientes de 9.190 usuarios[12].

Para conformar la muestra de análisis y subir contenidos a la plataforma Cyberelections Spain, Maldita.es asignó manualmente etiquetas basadas en palabras clave, o *keywords*. Por ejemplo, entre las etiquetas que se crearon para categorizar estos contenidos están "elecciones 23J", "elecciones 28M", "censo electoral", "actas electorales", "papeletas", "robo de votos", "voto por correo", "ley electoral", etc. Luego, el medio verificador creó tarjetas de contenido donde agrupó los observables en función del tema o asunto al que se referían. Esta selección identificó 139 casos de desinformación relacionados con el proceso electoral. Durante el análisis, otros 15 casos fueron descartados de la muestra: entre ellos, se encontraban casos no verificados por Maldita.es que resultaban imposibles de desmentir por el equipo de codificadores, o preguntas sobre el proceso electoral que los mismos usuarios enviaron a través del *chatbot*, pero que no estaban asociadas a un bulo[13]. De esta manera, la muestra final estuvo conformada por 124 casos.

3.2. Metodología de análisis y codificación

Las 124 tarjetas fueron analizadas por 10 alumnos del Máster de Políticas Públicas y Sociales de la Barcelona School of Management de la Universidad Pompeu Fabra[14]. La codificación de las categorías siguió la metodología del Observatorio Complutense de Desinformación, que, como se ha dicho, es una adaptación de la taxonomía FIMI, contenida en el informe EEAS del Servicio de Acción Exterior de la Unión Europea[15]. Los codificadores fueron entrenados a partir del libro de códigos desarrollado por el equipo de investigadores, sin la realización de un *test* de ICA (*intercoder agreement*) o ICR (*intercoder reliability*).

La taxonomía FIMI distingue primeramente los incidentes de los observables. El primer concepto se refiere a los eventos específicos en los que actores nacionales o extranjeros realizan interferencia y manipulación de información con el objetivo de influir en la percepción, opinión pública, políticas o procesos democráticos en un país objetivo, crean-

9 Libro de códigos disponible en la web del Observatorio Complutense de Desinformación, en el siguiente enlace: https://www.ucm.es/observatoriodesinformacion/observacion_electoral

10 El *chatbot* de WhatsApp fue lanzado en junio de 2020. Más información y detalles sobre este sistema pueden encontrarse en el siguiente enlace, consultado el 21 de junio de 2024: https://maldita.es/recibe-los-desmentidos-de-maldito-bulo-en-whatsapp/

11 Metodología de Maldito Bulo, disponible en el siguiente enlace (consultado el 26 de noviembre de 2024): https://maldita.es/metodologia-de-maldito-bulo/

12 Esto significa que el medio verificador recibió miles de potenciales casos de desinformación, aunque muchos de ellos eran repeticiones del mismo caso enviadas por diferentes usuarios, en formatos o plataformas también diferentes. Es importante mencionar que la repetición de un mismo caso en varias plataformas y formatos es sumamente relevante para el medio verificador, ya que es un indicador de viralidad.

13 Por ejemplo, una de las tarjetas indica que el 31 de mayo de 2023, un usuario envió al WhatsApp de Maldita.es la siguiente pregunta: ¿Cuál es la diferencia entre apoderado e interventor? Esta tarjeta fue descartada de la muestra, ya que se trata de una pregunta ciudadana destinada a entender el proceso electoral y no es, estrictamente, un caso de desinformación que pueda ser analizado bajo los parámetros de este estudio.

14 Leanna Zúñiga, Eugenia Hernández, Laura Henao, Daniel Iglesias, Linda Velásquez, Giannina Meléndez, Matías Zúñiga, Fernando Martínez, José Antonio Sánchez, Alfredo González La coordinación del equipo de codificadores y la formación sobre la metodología FIMI estuvo a cargo de los autores de este artículo.

15 La taxonomía FIMI fue desarrollada y presentada por el Servicio Exterior de la Unión Europea en febrero de 2023, a través del informe titulado "1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence". En este informe, el Servicio Exterior de la UE aplica la mentada taxonomía a algunos casos seleccionados de intervención y manipulación de la información provenientes de la órbita de propaganda e influencia rusa. El informe está disponible en el siguiente enlace: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

do narrativas de desinformación. Estos incidentes pueden involucrar la difusión de información errónea, desinformación, propaganda, operaciones de *hackeo* y filtración, y otras tácticas de manipulación para desestabilizar o influir en el entorno de información y política. Por otro lado, los observables son los elementos concretos a través de los cuales se desarrolló un incidente FIMI. Un incidente puede estar compuesto de varios observables. Por ejemplo, un mismo bulo puede distribuirse a través de un post de X, un video en TikTok y un *reel* de Instagram.

Seguidamente, la taxonomía FIMI busca identificar los siguientes elementos para cada observable: Objetivo; Canal en cuanto a su grado de relación con el Estado; Destinatario del ataque; Actor causante; Reacciones y medidas; Responsable de las medidas y Formato de las medidas. Un mayor detalle sobre estas categorías y sus respectivas opciones está en la Tabla 1.

Tabla 1. Categorías de la metodología FIMI bajo la que se analizó cada observable en la misión de observación electoral en España[16]

Nombre de la categoría	Tipo	Descripción
Objetivo	Variables	Presunto objetivo detrás del contenido desinformador. Admite selección múltiple. Las variables son: distraer, distorsionar, dividir, descartar, desalentar.
Canal en cuanto a su grado de relación con el Estado	Variables	Naturaleza del canal por el que se distribuye el contenido desinformador, en cuanto a su relación con el Estado. Admite selección múltiple. Las variables son: Canales oficiales de comunicación, Canales controlados por el Estado, Canales vinculados al Estado, Canales no atribuidos.
Destinatario del ataque	Variables	Persona y/o institución sobre la que trata el contenido desinformador y que, por lo tanto, es destinatario del ataque. Admite selección múltiple. Las variables son: Individuo; Órgano electoral; Gobierno; Instituciones del Estado y Actor político.
Actor causante	Variables	Identificación y enumeración de todas las personas y/o instituciones que emiten y/o difunden el contenido desinformador. Admite selección múltiple. Las variables son: Agente político, Medio de comunicación; Partido Político; Tercer actor.
Reacciones y medidas	Variables	Enumeración de todas las respuestas o reacciones ante el contenido desinformador. Admite selección múltiple. Las variables son: Declaración de refutación, Desacreditación, Contenido eliminado, Ninguno, Otro.
Responsable de las medidas	Variables	Identificación de el o los actores responsables de responder al contenido desinformador. Admite selección múltiple. Las variables son: Órgano electoral, Plataforma, Medio verificador, Instituciones del Estado, Actor político, Otro.
Formato de las medidas	Variables	Identificación del formato en que se emite la respuesta y/o reacción al contenido desinformador. Admite selección múltiple. Las variables son: Cadena de WhatsApp, Video, Imagen, URL, Artículo, Tweet, Audio, Post de Facebook, Story de Instagram, Telegram, SMS, Otro.

Finalmente, la plataforma Cyberelections Spain –desarrollada por Maldita.es– está integrada con una herramienta que, utilizando inteligencia artificial, agrupa las tarjetas en *clústeres* para identificar narrativas y metanarrativas: las narrativas son la asociación de las diferentes fichas en un solo objetivo, mientras que las metanarrativas son la interpretación máxima, concreta y directa de lo que busca la I*nterferencia y Manipulación de la Información.* Las 124 tarjetas de contenido cumplían con las condiciones técnicas para poder implementar la herramienta[17], y lograron agruparse 41 narrativas y 13 metanarrativas.

4 Análisis y resultados

Antes de exponer los hallazgos principales, es importante recordar que las categorías confeccionadas para esta metodología admiten selección múltiple: se solapan y no son mutuamente excluyentes. Esto significa que un mismo observable puede haberse replicado por diferentes plataformas, apuntado a varios destinatarios o perseguido varios objetivos. Por ejemplo, un observable puede haberse difundido por WhatsApp y X, atacando –al mismo tiempo– a un ministro de gobierno y al órgano electoral, con el objetivo de distorsionar la realidad y

16 Es menester mencionar que en el marco de este proyecto se han realizado 14 misiones de observación electoral, con las que se ha refinado el método. Luego de la observación en España, las categorías fueron modificadas para ajustarse mejor al contexto de las elecciones de 2024, añadiendo opciones relevantes a nivel local. Por ejemplo, en destinatario del ataque se añadieron las opciones de candidato o candidata; empresa proveedora del Estado, partido político y tercer actor. La versión más actualizada de esta metodología se encuentra en el sitio web del Observatorio Complutense de Desinformación: https://www.ucm.es/observatoriodesinformacion/observacion_electoral

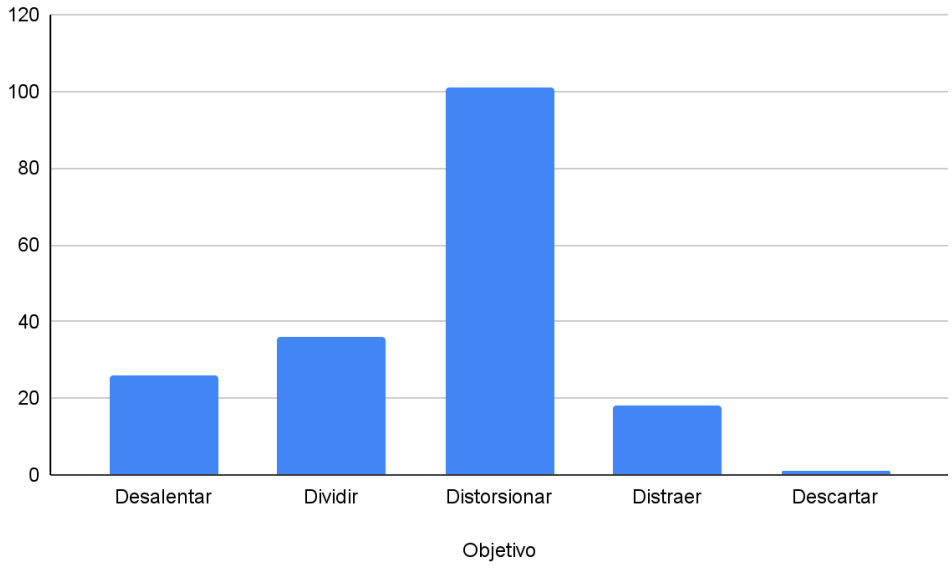
17 Para que funcione correctamente la Inteligencia Artificial de la plataforma Cyberelections, cada tarjeta de contenido debía cumplir con las determinaciones técnicas necesarias. El principal requisito era que tanto el título de la tarjeta como el recuadro del contenido tuvieran información descriptiva del caso de desinformación. Según indica el manual de títulos y contenidos elaborado por Maldita.es para el correcto uso de la plataforma, “el título de la tarjeta debe ser una frase sencilla que describa la parte más esencial del contenido, es decir, el mensaje que se transmite. No debe entenderse el título como una serie de palabras clave inconexas, sino como una oración estructurada que represente unívocamente el contenido y la intención del mensaje, sin hacer juicio de valor o juzgar de antemano si se trata de un bulo o no”. En cuanto al recuadro de contenido, éste debía completarse con “una descripción de los mensajes potencialmente desinformadores”, sin hacer una valoración del contenido.

dividir a la sociedad. La selección múltiple permite, precisamente, recoger las distintas características que describen a un observable y refleja el carácter de los mismos a través de varias dimensiones. Los datos que se presentarán a continuación indican la frecuencia de aparición de cada variable.

4.1. Objetivos de la desinformación

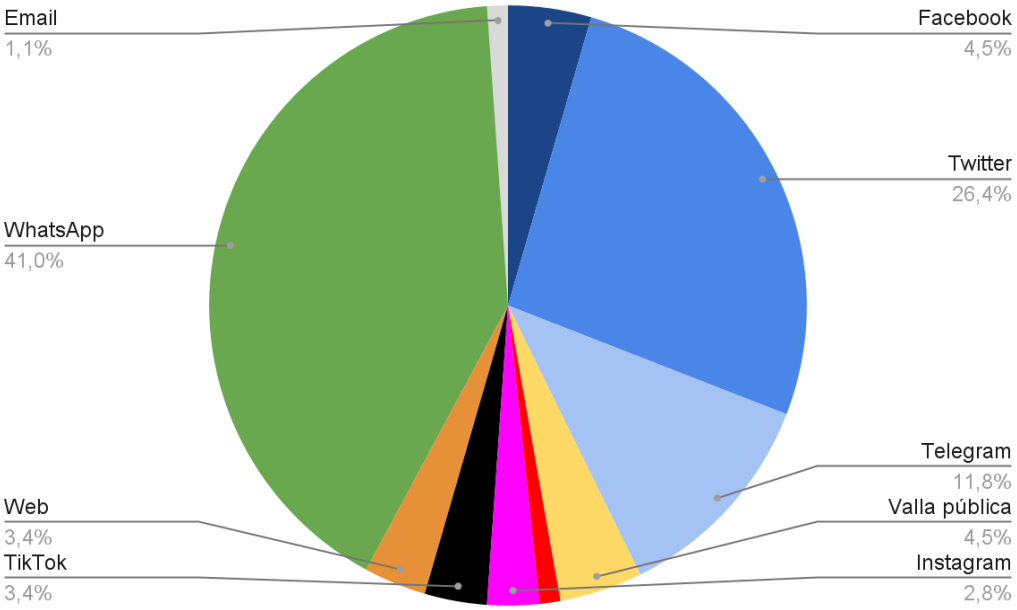
Entre los principales objetivos de los bulos electorales está "distorsionar" que, según la metodología de esta investigación, implica la acción de "cambiar el marco, retorcer y modificar el sentido de la realidad". 101 de los 124 casos analizados en España parecen perseguir este objetivo (ver Figura 1). Le sigue "dividir", con 36 casos, entendido como el propósito de "crear conflictos o ampliar las divisiones dentro o entre comunidades y grupos".

Figura 1. Frecuencia de objetivos



Fuente: Elaboración propia a partir del análisis y codificación de observables

Figura 2. **Frecuencia de origen de los observables**



Fuente: Elaboración propia a partir del análisis y codificación de observables.

4.2. Medios de distribución de la desinformación

A partir del análisis de estos 124 casos de desinformación, se puede concluir que Whatsapp fue el principal medio de distribución de los casos de desinformación en España. 73 de 124 casos (41%) incluyen a esta plataforma de mensajería instantánea como canal, lo que no quiere decir que no se haya difundido simultáneamente por otras vías. El siguiente canal de origen, por orden de frecuencia

de aparición, es X (ex Twitter), siendo el canal de distribución de 47 (26,4%) observables. En tercer lugar, la plataforma Telegram, con 21 (11,8%) observables.

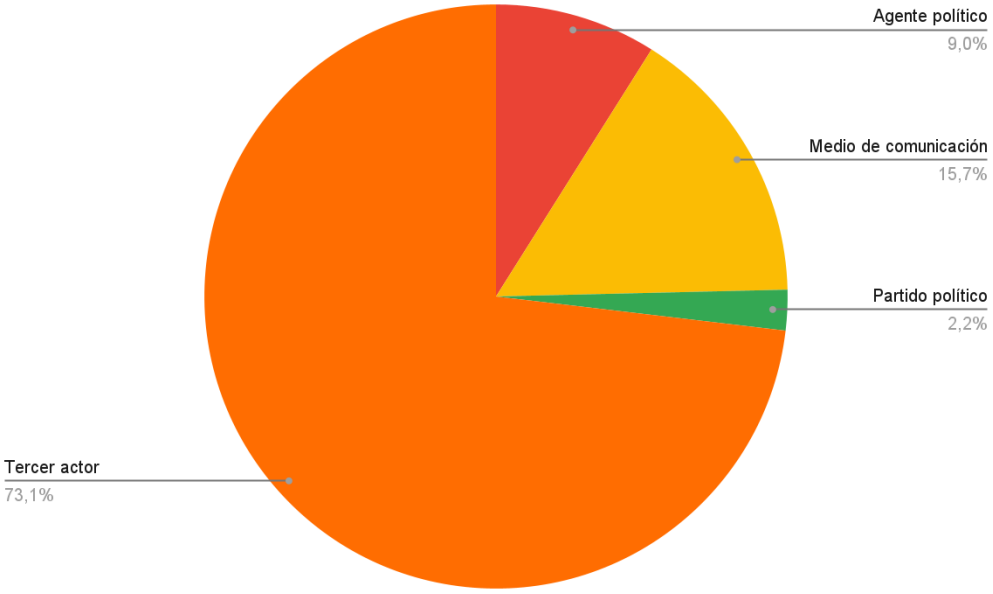
4.3. Actores causantes de la desinformación

El principal actor causante de la desinformación electoral fue un Tercer actor, mencionado en 98 casos (73,1%). Tercer actor corresponde al que no coincide con ninguna de las otras categorías, que en este caso eran Medio de Comunicación (21 casos), Agente Político (12 casos) y Partido Político (3 casos).

4.4. Destinatarios de la desinformación

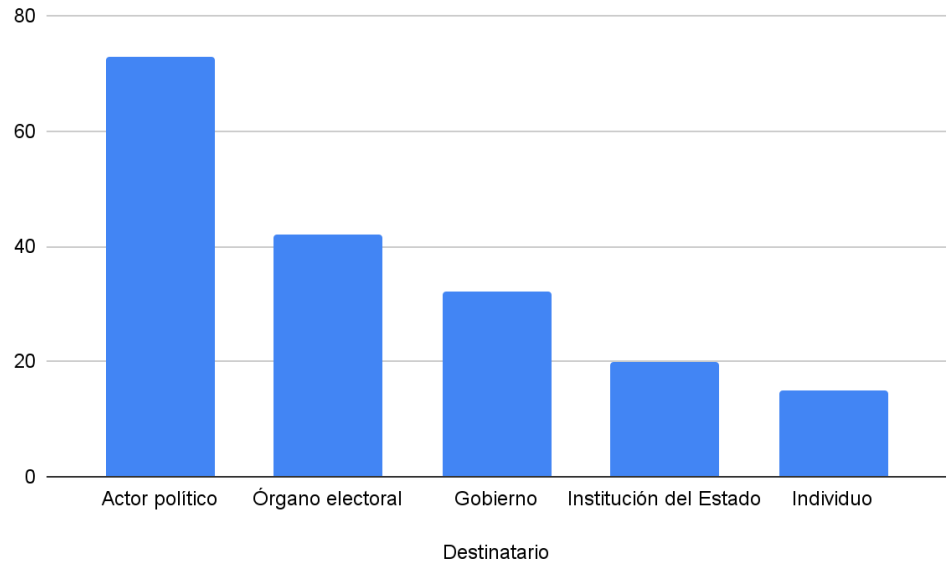
Entre los principales destinatarios de los ataques de desinformación están actores políticos (73 casos lo mencionan), el/los órganos electorales (42 casos lo(s) mencionan) y el gobierno (32 casos lo mencionan). Este hallazgo es significativo ya que aporta evidencia de que los órganos de la administración electoral –que en España corresponden a la Junta Electoral Central, las Juntas Electorales Provinciales y las Juntas de Zona– son destinatarios frecuentes de los ataques de desinformación.

Figura 3. Frecuencia de actor causante



Fuente: Elaboración propia a partir del análisis y codificación de observables.

Figura 4. Frecuencia de destinatarios



Fuente: Elaboración propia a partir del análisis y codificación de observables.

4.5. Narrativas y metanarrativas de desinformación

La plataforma Cyberelections logró consolidar 41 narrativas extraídas de las 124 fichas. Esas 41 narrativas se unificaron en 13 metanarrativas. La Tabla 2 muestra el resultado de esa unificación.

Tabla 2. Recuento de las metanarrativas de desinformación que circularon en las elecciones españolas de 2023

	Metanarrativa	Recuento
1	Los políticos aumentan privilegios y cargos sin importar el partido.	2
2	Pedro Sánchez busca una salida personal adelantando elecciones y dimitiendo como secretario general del PSOE.	2
3	El PSOE busca votos de inmigrantes en mezquitas a cambio de ayudas	3
4	El Rey de Marruecos influye en las elecciones españolas a favor del PSOE.	2
5	Grupos utilizan la frase 'que te vote Txapote' en lugares públicos para provocar o hacer una declaración política	3
6	Sánchez e Indra manipulan el voto por correo para alterar los resultados electorales	4
7	El gobierno manipula el censo electoral para cometer fraude en las elecciones de Huelva.	2
8	El gobierno manipula el proceso electoral a través del voto de extranjeros.	3
9	Indra y el gobierno manipulan los resultados de las elecciones del 23-J	4
10	Correos y la Junta Electoral facilitan fraude electoral al no exigir DNI para votar.	5
11	El gobierno de Sánchez y Correos están involucrados en un fraude electoral en las elecciones del 23-J.	5
12	El presidente de Correos manipula el voto por correo en secreto	4
13	Felipe VI y Ursula von der Leyen intervienen en la política española para influir en el resultado electoral	2
		41

Fuente: Elaboración propia a partir de los resultados arrojados por la inteligencia artificial de Maldita.es

De estas 13 metanarrativas y su frecuencia, destacan los siguientes elementos que también permiten vincular a las metanarrativas entre sí:

- Fueron comunes las narrativas que se refieren al voto por correo, una modalidad de votación que fue particularmente relevante durante las elecciones generales de julio de 2023 (por coincidir con la época de verano y vacaciones). Las narrativas de desinformación que se refieren al voto por correo apuntan a dos supuestas situaciones alarmantes: 1) que el gobierno (encabezado por Pedro Sánchez, del PSOE) habría manipulado el resultado a través de esta modalidad de votación (metanarrativas 11 y 12); 2) que el órgano electoral habría permitido o facilitado un fraude a través de esta modalidad de votación (metanarrativa 10).
- Fueron comunes las narrativas que se refieren a INDRA[18] (metanarrativas 6 y 9), una empresa de consultoría y tecnología que ha obtenido la adjudicación de contratos con el Estado para proveer servicios tecnológicos a diferentes órganos y servicios. Los contenidos de desinformación apuntan, sin fundamento, a que INDRA, en concomitancia con el gobierno, ha manipulado los resultados de las elecciones a través del conteo de votos. Medios de comunicación y *fact-checkers* han publicado en numerosas ocasiones artículos que se refieren al rol de INDRA en las elecciones[19] dando cuenta de que es un bulo recurrente. En estos artículos, los medios verificadores aclaran que el rol de INDRA se limita a proveer la infraestructura tecnológica para unificar los datos provisionales enviados por la administración electoral –que es la verdadera encargada del conteo de votos– y posteriormente difundirlos.
- Fueron comunes las narrativas que se refieren a migrantes, apuntando que una de las candidaturas estaría buscando activamente su voto a través de ayudas y beneficios (metanarrativa 3). Entre estas narrativas, se detectan también aquellas que apuntan a una supuesta injerencia de autoridades y/o figuras del mundo árabe en las elecciones, en favor de la lista de gobierno (metanarrativa 4). Estas metanarrativas tienen un hilo común en sugerir que los migrantes o los extranjeros de ciertos países son dignos de desconfianza o sospecha.
- Fueron comunes las narrativas que apuntaban a que el partido político/coalición política que está en el gobierno –y personalmente, el presidente de gobierno en el cargo– es causante de situaciones alarmantes, como manipulación y fraude electoral. Las narrativas que señalaban a los políticos "en general" fueron marginales, mientras que la mayor parte de los casos de desinformación indicaba que el gobierno de turno, con supuesto acceso a influir en diferentes organismos del Estado, fue el responsable de acciones que afectan la integridad del proceso electoral (metanarrativas 2, 3, 4, 6, 7, 8, 9 y 11).

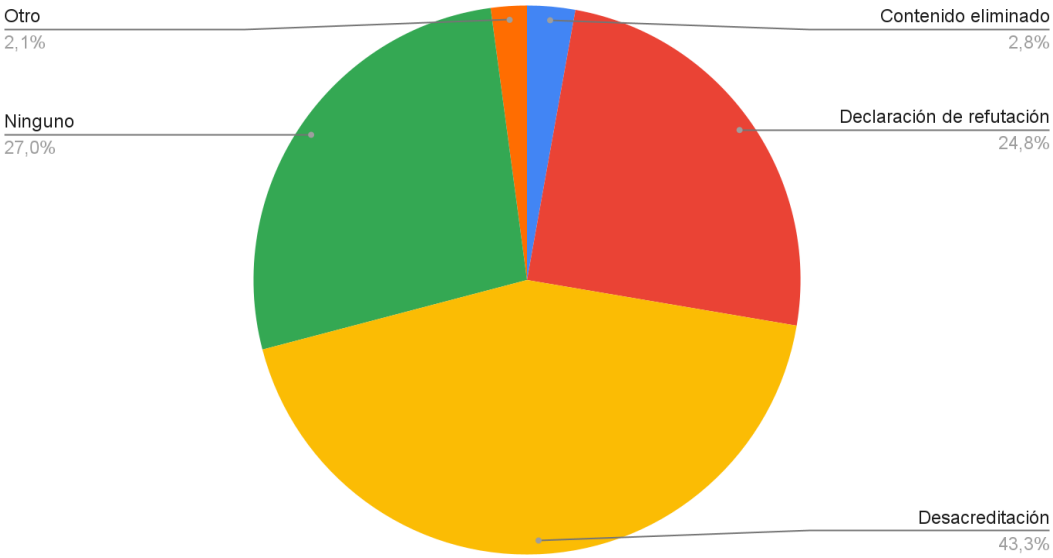
18 Ver la web de la empresa en el siguiente enlace: https://www.indracompany.com/

19 Por ejemplo, ver los siguientes artículos:
Maldita.es, de julio de 2022: https://maldita.es/malditobulo/20220701/indra-empresa-recuenta-votos-elecciones/
Newtral, de junio de 2022: https://www.newtral.es/indra-recuento-votos-elecciones-gestion-transmision-datos/20220629/
Cadena SER, de julio de 2023: https://cadenaser.com/nacional/2023/07/05/las-desinformaciones-sobre-indra-y-las-elecciones-en-espana-cadena-ser/
EFE Verifica, de mayo de 2023: https://verifica.efe.com/recuento-votos-espana-se-hace-a-mano-en-cada-mesa-electoral-sin-intermediarios/

4.6. Reacciones y medidas adoptadas

En cuanto a las medidas y/o reacciones como respuesta a los incidentes de desinformación durante las elecciones españolas de 2023, los resultados de este estudio muestran que la principal medida fue la desacreditación de medios verificadores. Un 43,3% de los casos fue investigado y desacreditado a través del *fact-checking*.

Figura 5. Frecuencia de reacciones y medidas



Fuente: Elaboración propia a partir del análisis y codificación de observables.

Entre estos resultados destaca que la segunda reacción o medida más frecuente fue "Ninguno" (27%). Es decir, de los 124 casos de desinformación cargados en la plataforma Cyberelections, en 38 no existe evidencia de que se hayan tomado medidas de ningún tipo, lo que abrió la posibilidad a que este contenido falso circulara libremente por las plataformas, sin contar tampoco con una reacción de la sociedad civil (como puede ser el desmentido de un medio verificador) ni de las instituciones del Estado (como, por ejemplo, un comunicado o una refutación del órgano electoral). A pesar de esto, es cierto que la declaración de refutación del actor involucrado, como el órgano electoral o el actor político, representó un 24,8% de las reacciones[20]

Para finalizar, destaca también que, según la evidencia obtenida, la eliminación de contenidos de las plataformas de redes sociales, como Facebook o Twitter (ahora X), según la evidencia recogida, ha sido marginal. Sólo en 4 de los 124 casos (2,8%) se pudo verificar que se eliminó el contenido de las plataformas.

5. Discusión

En un contexto de campañas y procesos electorales de alto riesgo (Rubio-Núñez et al, 2024), en donde la desinformación busca socavar la confianza de la ciudadanía en las instituciones democráticas (Sivalo, 2024; McKay & Tenove, 2021), este ejercicio de observación electoral recolectó evidencia del fenómeno en el marco de las elecciones españolas de 2023, considerando las municipales y autonómicas de mayo y las generales de julio. Los resultados confirman lo que había sido identificado por medios verificadores y organizaciones de la sociedad civil: que existió "una operación de desinformación clara y sostenida para deslegitimar la integridad del sistema electoral español y socavar la confianza pública en unas elecciones libres y justas en el país" (Fernández, 2024, p.196)[21]. En este sentido, vale la pena mencio-

20 En relación con estos resultados, resulta relevante contrastarlos con las medidas tomadas por la Junta Electoral Central y las Juntas Provinciales de España en el contexto de las elecciones de 2023, que, aunque no hayan sido directamente recogidas a través de este análisis FIMI, son de conocimiento público. Las reacciones y medidas adoptadas por dichas autoridades, en el marco de sus competencias y facultades, tuvieron un papel fundamental para salvaguardar el desarrollo correcto de los comicios (Corredoira y Alfonso, 2024). El número de incidencias que han sido revisadas por la JEC y las juntas provinciales son relativamente pocas, pues estas autoridades actúan a instancia de parte, lo que limita necesariamente el número de casos en los que intervienen directamente. Sin embargo, se identifican los siguientes acuerdos de la JEC, pues son una muestra relevante del trabajo de las autoridades por defender el proceso electoral:
1. Acuerdo JEC 513/2023, del 20 de julio, sobre no establecer medidas adicionales respecto al voto por correo. Disponible en: https://www.juntaelectoralcentral.es/cs/jec/doctrina/acuerdos?anyosesion=2023&idacuerdoinstruccion=122169&idsesion=1047&template=Doctrina/JEC_Detalle
2. Acuerdo JEC 503/2023, del 12 de julio, que reitera su doctrina garante de la libertad de expresión y descarta censurar propaganda electoral que incorpora el himno franquista "Cara al Sol". Disponible en: https://www.juntaelectoralcentral.es/cs/jec/doctrina/acuerdos?anyosesion=2023&idacuerdoinstruccion=121373&idsesion=1046&template=Doctrina/JEC_Detalle
3. Acuerdo JEC 525/2023, del 20 de julio, sobre las limitaciones establecidas en el artículo 66 de la LOREG, que no afectan a periódicos digitales como OKDirario. Disponible en: https://www.juntaelectoralcentral.es/cs/jec/doctrina/acuerdos?anyosesion=2023&idacuerdoinstruccion=121768&idsesion=1047&template=Doctrina/JEC_Detalle

21 Fernández (2024) se refiere a un informe elaborado por Maldita.es en conjunto con Democracy Reporting International, donde analizaron los bulos que circularon durante el mes previo a las elecciones generales del 23 de julio. El informe está disponible en el siguiente enlace (en inglés): https://democracyreporting.s3.eu-central-1.amazonaws.com/images/6509b182b6569.pdf

nar que, si bien este estudio reúne evidencia de 124 casos de desinformación electoral, no ha probado que estos esfuerzos de engañar y manipular hayan estado coordinados entre sí.

Consecuentemente, se analizarán tres grupos de resultados, en donde se dialogará con la literatura y se aportarán recomendaciones para combatir la desinformación, basadas en la evidencia presentada en el estudio:

5.1. Sobre el contenido desinformador y sus objetivos

De acuerdo con lo observado, los principales destinatarios de ataques de desinformación son los actores políticos y los órganos electorales, con el objetivo de dañar la confianza en el proceso. Esto confirma lo indicado por la literatura, respecto a que lo que se busca con la desinformación en periodo electoral no es tanto modificar la intención de voto –que según Syrovátka, Hořejš & Komasová (2023) es una decisión que está instalada previamente a la exposición a contenido desinformador– sino deslegitimar el sistema democrático y sus instituciones en general (McKay & Tenove, 2021).

En consecuencia, y de acuerdo con lo observado, en la mayoría de los casos (101 de 124) el principal objetivo que persiguen los ataques es "distorsionar" el sentido de la realidad. Esto da pistas sobre qué tipo de medidas contra la desinformación pueden ser efectivas: precisamente aquellas que buscan informar sobre el proceso y el sistema, y que puedan contrarrestar los intentos de distorsión o deslegitimación. En ese sentido, las medidas preventivas, tales como entregar información a la sociedad sobre el funcionamiento del proceso electoral son claves. Si los ciudadanos no conocen o no entienden el sistema, sus actores, sus competencias y facultades, son más vulnerables a los intentos de manipulación para hacerles creer que el proceso está siendo vulnerado y que la elección es ilegítima, lo que finalmente interfiere con su derecho a voto y con su participación electoral plena.

Lo anterior se corrobora con el análisis de metanarrativas hecho a través de la plataforma Cyberelections. Las metanarrativas más comunes se refieren al voto por correo e intentan hacer creer a la ciudadanía que los resultados se manipulan a través de dicha modalidad de votación. Esta desinformación busca minar la confianza en el sistema que administra y gestiona el voto por correo, cuando en realidad, su objetivo es garantizar que más ciudadanos puedan ejercer su derecho a sufragio.

Las narrativas que hacen sospechar de diversas etapas del proceso y de actores legítimos (como proveedores) que participan en él también fueron comunes. En ese sentido, es importante que autoridades y proveedores sean transparentes sobre su papel en el proceso, qué tipo de servicio se presta y para qué sirve. **En definitiva, es esencial que la ciudadanía esté enterada de qué funciones pueden y deben cumplir estos proveedores y –sobre todo– qué funciones están fuera de sus competencias.** Por ejemplo, en el caso español es importante reforzar la información sobre el rol de la empresa INDRA, que se limita solamente a proveer de una solución tecnológica para unificar y diseminar los resultados provisionales de la elección, cuyo origen es de hecho la autoridad electoral, la única encargada del conteo de los votos.

También fueron comunes las narrativas que culpan al partido en el gobierno de turno como causante de la manipulación del voto y el fraude electoral. Esto no solo es consecuente con los intentos de manipulación antes descritos, sino que también refleja la "importación" de este tipo de narrativas de contextos electorales distintos (e.g. las elecciones de EE.UU. de 2020, donde se alegó falsamente que el gobierno de turno manipuló el resultado de las elecciones).

El análisis también evidenció que, entre las narrativas más comunes está la supuesta evidencia de que los colectivos migrantes o sus países de origen interfieren en los procesos electorales. Esto podría apuntar que existe también una correlación entre las narrativas xenófobas y las que buscan atacar el proceso electoral, o, dicho de otra manera, que se instrumentaliza la xenofobia para alentar las dudas sobre la legitimidad del proceso. Nuevamente, esto es consecuente con narrativas que se han observado en países extranjeros como Estados Unidos, donde el bulo de que los inmigrantes irregulares votan en las elecciones es recurrente.

Lo anterior apunta a que las autoridades y otras organizaciones que colaboran en la lucha contra la desinformación deben estar atentos a las narrativas que se usan en otros contextos electorales, las que parecen ser "contagiosas". Saber qué ha pasado en otros lugares del mundo con anterioridad puede ser útil para preparar los posibles escenarios y las posibles respuestas en un contexto posterior.

5.2. Sobre los medios de distribución de la desinformación

Los resultados de esta observación indican que el principal canal de distribución en las elecciones españolas de 2023 fue Whatsapp. Un 59% de los casos fueron distribuidos a través de esta plataforma. Los siguientes canales más populares fueron Twitter (26,4%) y Telegram (11,8%). Respecto a este hallazgo, es importante mencionar que la prevalencia de Whatsapp puede estar determinada por el *chatbot* implementado por Maldita.es. El medio verificador ha obtenido gran parte de los casos que posteriormente investiga y verifica a través de esa vía, lo que puede explicar por qué se reflejan un mayor número de casos. Sin embargo, es interesante que este resultado dialoga con el Digital News Report 2023, del Instituto Reuters, que también identifica a WhatsApp como la aplicación de mensajería más utilizada en España. Un 79% de los encuestados declaran usarla para todo fin (por sobre Facebook, YouTube e Instagram) y un 27% declara utilizarla para consumir noticias (Reuters Institute for the Study of Journalism, 2023).

Así, la prevalencia de Whatsapp como canal de origen de casos de desinformación electoral se debe al alto nivel de utilización de dicha aplicación y también ayuda a explicar por qué Maldita.es tomó la decisión de implementar el *chatbot* en dicha plataforma: es merecedora de más atención con base en su popularidad entre los usuarios. Los desinformadores también lo saben y explotan dicha popu-

laridad. De lo anterior se desprende que es necesario que aquellos que se dediquen a luchar contra la desinformación (autoridades, periodistas, sociedad civil, etc.) **estén atentos a los canales que son más populares en momentos y contextos determinados, en particular durante períodos electorales, y preparen respuestas adecuadas que puedan llegar a los usuarios de los canales más populares de manera prioritaria.**

Respecto a las medidas adoptadas, los resultados indican que la principal medida es la desacreditación, es decir, la constatación de que el contenido es falso o manipulado. Esta fue la medida adoptada en un 43,3% de los casos. Es importante destacar que este hallazgo no fue inesperado, ya que seguramente está influenciado por la fuente desde donde se obtienen los casos de desinformación, que corresponde a un medio verificador. Sí fue más sorprendente que la medida de "eliminación o restricción del contenido" en la plataforma se haya adoptado sólo en un 2,8% de los casos y que en un 27% no se haya tomado medida alguna.

Como un aporte a la discusión, creemos que este resultado se debe a tres posibles escenarios:

El primer escenario es que a pesar del esfuerzo de los *fact-checkers* por corregir la desinformación, las plataformas no aprovechan ese trabajo para eliminar o restringir todos los contenidos corroborados como información falsa o distorsionada. Esto puede deberse a que las plataformas prefieren utilizar el trabajo de los *fact-checkers* para poner en contexto información posiblemente falsa y dejan en manos del ciudadano ejercer su responsabilidad y decidir por sí mismo con base en la información disponible. Esta reacción no deja de ser positiva en un contexto democrático. También contribuye a que las plataformas eviten la censura desmedida.

El segundo escenario, y así lo evidencia el que no se haya podido registrar ningún tipo de acción sobre un 27% de los casos, es que entre todos los actores involucrados no hay la suficiente capacidad de atender y corregir todas las instancias de desinformación que suceden. Aunque la información con la que contamos no permite afirmar esto con contundencia (ya que este no es un estudio que mida el volumen de la desinformación circulante), de poder probarse, este escenario debería ser motivo de preocupación e indicador de que hace falta mejorar la capacidad de respuesta.

El tercer escenario es que el bajo número de casos identificados como "contenido eliminado" y el alto número de casos en donde no se tomó ninguna acción se deba a que no pudimos verlo. Aunque hicimos un seguimiento a cada uno de los bulos, es posible que la información simplemente no sea accesible o no esté disponible. Es decir, **las plataformas de redes sociales no son suficientemente transparentes a la hora de informar qué tipos de acciones han tomado sobre los contenidos desinformadores, siendo esto indicador de que hacen falta mayores esfuerzos de transparencia y cooperación entre plataformas, autoridades y organizaciones de la sociedad civil que luchan contra la desinformación**[22]

El Reglamento de Servicios Digitales (DSA) incluye una herramienta poderosa contra la desinformación en las obligaciones de monitorización y mitigación de riesgos sistémicos, que impone a las plataformas que cumplen ciertos requisitos en cuanto al número de usuarios (las así llamadas Plataformas de Muy Gran Tamaño o VLOPs en inglés), siendo el criterio la vinculación del tamaño de las plataformas con el riesgo de daños sociales y económicos para la sociedad (Broughton Micova, 2021).

Desafortunadamente, las reglas de la DSA están dirigidas a riesgos asociados con la amplificación algorítmica de contenido dañino, y a la moderación de contenidos compartidos a través de redes públicas, por lo que los canales privados de servicios de mensajería como WhatsApp o Telegram no encajan en la definición de VLOPs y por lo tanto están exentas de estos requerimientos (Cetina-Presuel, 2024b). La nueva ley europea no da herramientas para combatir la desinformación en entornos de comunicación privada por sí solos, aunque sí contempla protecciones cuando estos contenidos se comunican públicamente en otras redes digitales. De hecho, según el último reporte de transparencia enviado a la Comisión Europea, el servicio de *WhatsApp Channels* (canales públicos) tiene un promedio de 46.8 millones de usuarios[23] **Por lo tanto, la plataforma será considerada una VLOP y tendrá que seguir el máximo de obligaciones posibles según la DSA, incluyendo las medidas contra riesgos sistémicos, entre ellos la desinformación.** Esto es una buena noticia para entender cómo estos fenómenos funcionan en red y desarrollar medidas que permitan inocular a las redes públicas de lo que se comparte en privado. Mucho de eso pasará por la detección temprana de contenidos.

Por supuesto, la DSA seguirá teniendo el punto ciego de los canales privados. Hay que tener en cuenta que cualquier intervención legislativa sólo podrá centrarse en monitorizar y minimizar riesgos en el momento en que la información salte de un canal privado a un entorno público. De lo contrario, podría haber un impacto negativo en la libertad de expresión. Una avenida a explorar es tener en cuen-

22 Es importante destacar que la base de datos, poblada con ejemplos proveídos por un *fact-checker*, no siempre permite determinar si se ha tomado algún tipo de medida o no si la información no se encuentra en el ejemplo concreto. Esto es en parte por cómo opera la actividad *fact-checking* en sí (que intenta impedir que el bulo siga circulando), y en parte porque las plataformas no siempre son transparentes respecto de las medidas que se toman o no se toman. Sobre esto último, la DSA europea ha de mejorar el panorama por lo menos en algunos aspectos si logra superar las barreras identificadas respecto de su cumplimiento pleno. Al respecto, véase Strowel & de Meyere (2023). Además, algunas de las prácticas de las plataformas en cuanto a moderación de contenidos, si bien pueden ser efectivas, también pueden resultar menos transparentes. Un claro ejemplo de esto es el *shadowbanning*, que es una alternativa al bloqueo o eliminación de contenidos mediante la limitación de su circulación mediante el algoritmo, pero generalmente sin el conocimiento del afectado, lo que evidentemente afecta no solo a la mencionada transparencia, sino también posiblemente al derecho que tendrá el afectado a interponer recurso o recurrir al arbitraje. Para una discusión sobre el encaje del *shadowbanning* en la DSA véase a Leersen (2023).

23 Véase el artículo "WhatsApp is now a Very Large platform in the EU, and will face tougher regulation", en The Verge. Disponible en el siguiente enlace: https://www.theverge.com/news/614445/whatsapp-channels-very-large-platform-vlop-digital-services-act-eu

ta el potencial impacto del tamaño de un servicio como WhatsApp con base en el número de usuarios y considerar esto como un factor de riesgo que facilita el paso de la desinformación de un sistema de mensajería privado a una red social pública para establecer un mecanismo de monitorización respecto de este "trasvase". Tal vez esto se ajuste mejor a la realidad de los distintos tipos de servicios digitales y los riesgos que representan.

Enmiendas legislativas aparte, es de suma importancia continuar haciendo observaciones empíricas que corroboren que la desinformación más nociva se distribuye también por otros canales que no entran en las categorías establecidas por la DSA.

5.3. Sobre las reacciones y medidas

Según los resultados de esta observación, los órganos electorales o los actores políticos han hecho declaraciones de refutación directas sobre contenido desinformador en un 24,8% de los casos. **Esto es positivo, ya que en cuanto los ataques de desinformación apuntan a un sistema y sus procesos, la aclaración con información oficial –señalando las normas y leyes que lo regulan en un lenguaje claro– parece ser la mejor herramienta para hacer frente al incidente de desinformación en el momento.** Por ejemplo, en el mismo ejercicio de observación desarrollado en Estados Unidos, el equipo de investigación identificó rápidas reacciones de los órganos electorales en los llamados "swing states" (estados indecisos), que en el transcurso de pocas horas desde que comenzó a circular el bulo, publicaron comunicados declarando el contenido como falso y explicando por qué con información técnica y normativa (Corredoira & Gaete, 2024).

Es comprensible, sin embargo, que los órganos de la administración electoral no tengan la capacidad para responder directamente a todos los ataques que le implican. A ello hay que añadir que el número de incidencias que llegan efectivamente a las Juntas Electorales son muy pocas, ya que actúan a instancia de parte, y en su mayoría, o carecen de consistencia o sus emisores no son conocidos. Al respecto, Corredoira y Alfonso (2024) asegura que, aunque a la JEC le corresponde la vigilancia de todo el proceso de campaña electoral (de acuerdo con los artículos 42 y 50-53 de la LOREG), resulta indispensable "fortalecer el conjunto de las autoridades electorales ponderando los nuevos desafíos del derecho a la información" (p.235). Se necesita no sólo mayor dotación de personal, medios técnicos y de gestión para monitorizar los entornos virtuales, sino mayores garantías o sistemas de corregulación, "para que los novísimos medios no intercepten las campañas" (Corredoira y Alfonso, 2024, p.235). De la misma forma, se ha de exigir a las plataformas y a la sociedad civil que les ofrezcan toda la ayuda posible para este fin.

Por otro lado, según nuestro estudio, la eliminación de contenidos de las plataformas de redes sociales ha sido marginal (sólo 4 de 124 casos)[24] Si bien es cierto que esto podría ser señal de que las plataformas optan por medidas que no impliquen la retirada de contenido (como las etiquetas de contexto y otras técnicas ya discutidas), también invita a poner en cuestión si las medidas y acciones contra la desinformación de estas empresas son suficientes. Hemos de recordar que las plataformas están llamadas a colaborar no solo por responsabilidad social corporativa, sino porque la legislación europea se lo exige.

Es posible que las plataformas hayan tomado más medidas de las que hemos podido ver pues la falta de transparencia con la que operan es un problema al que nos enfrentamos. El artículo 15 de la DSA impone obligaciones de transparencia a los prestadores de servicios intermediarios, incluyendo la obligación de publicar al menos una vez al año informes sobre las actividades de moderación de contenidos realizadas durante dicho período, los que deben incluir información relevante sobre el tipo de medidas adoptadas que afecten "a la disponibilidad, visibilidad y accesibilidad de la información proporcionada por los destinatarios del servicio..." (art. 15.1 letra e de la DSA). Las plataformas también deben reportar sobre "el uso de medios automatizados con fines de moderación de contenidos, incluyendo una descripción cualitativa, una especificación de los fines precisos, los indicadores de la precisión y la posible tasa de error de los medios automatizados empleados para cumplir dichos fines, y las salvaguardias aplicadas" (art. 15.1 letra e de la DSA). Sin embargo, existen ciertas dudas sobre la efectividad de estas obligaciones de transparencia (Stowell & de Meyere, 2023). Además, en consonancia con la observación hecha líneas arriba, estas obligaciones nos permitirán entender mejor a las plataformas de comunicación pública, pero no dan herramientas para atender a los canales de comunicación privada por donde también circula desinformación, como Whatsapp o Telegram.

6. Conclusiones

El estudio de las elecciones españolas de 2023 evidencia que han circulado una variedad de categorías de desinformación encaminadas a deslegitimar el sistema democrático y a afectar la confianza pública en un proceso electoral libre y justo. Los datos recopilados revelan patrones de ataques dirigidos tanto a actores políticos como a órganos electorales, confirmando que el objetivo principal ha sido distorsionar la percepción del sistema y los organismos a cargo de la administración del proceso. El análisis de los canales de distribución destaca la prevalencia de aplicaciones de mensajería como WhatsApp y Telegram, que representan un desafío particular para la monitorización y mitiga-

24 Durante las municipales de mayo hubo un caso de eliminación o limitación de cuentas de redes sociales que, aunque está fuera de la muestra analizada en este estudio, es importante mencionarlo. Se trató del bloqueo que hizo Twitter de las cuentas de los candidatos de Unides Podem, Héctor Illueca y Pilar Lima, en Valencia, a una semana de las elecciones. Ver más información en el siguiente artículo: https://www.eldiario.es/comunitat-valenciana/twitter-bloquea-cuentas-candidatos-unides-podem-hector-illueca-pilar-lima_1_10223759.html

ción de la desinformación debido a su naturaleza privada, lo que evidencia potenciales limitaciones en nuevas leyes como la DSA. También demuestran que es absolutamente necesario seguir investigando la desinformación en estos entornos para entenderlos mejor.

Las medidas adoptadas por las autoridades competentes como la Junta Electoral Central, entre otros actores políticos y de gobierno, y de la sociedad civil, a través de *fact-checkers* como Maldita.es, sirven para confirmar que los esfuerzos de verificación y las declaraciones oficiales son fundamentales. No obstante, hace falta más trabajo para dotar a las autoridades e instituciones con mejores capacidades y herramientas para hacer frente a la desinformación de una manera más sistémica y proactiva. Para ello, la colaboración entre todos los actores relevantes –entre los que también hemos de incluir a los académicos– es indispensable.

Solo a través de esfuerzos colaborativos sostenidos se podrán entender con mayor precisión los desórdenes informativos y se podrán detectar y contrarrestar los efectos dañinos de la desinformación para las sociedades democráticas. Es urgente que esta colaboración también desarrolle estrategias para fortalecer la confianza de la ciudadanía en sus instituciones, sin duda una de las claves para salvaguardar la integridad de los procesos electorales.

Finalmente, es pertinente mencionar como limitación de este estudio que, aunque la metodología FIMI aplicada en esta misión de observación electoral proviene de una taxonomía validada por la comunidad internacional de ciberseguridad –y ha sido refinada por un equipo transnacional del Observatorio Complutense de Desinformación– el nivel de acuerdo de los codificadores no fue medido a través de tests ICR o ICA. El uso de estos tests es altamente recomendado para estudios cualitativos (O'Connor & Joffe, 2020) y debe tenerse en consideración para réplicas futuras de esta metodología.

7. Referencias

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication, 33(2), 122-139. https://doi.org/10.1177/0267323118760317

Broughton Micova, S. (2021) What is the Harm in Size: Very Large Online Platforms in the Digital Services Act. Centre for Regulation in Europe (CERRE). Recuperado de: https://ueaeprints.uea.ac.uk/id/eprint/83031/

Bustos-Gisbert, R. (2021). La formación libre de la opinión pública en la nueva sociedad tecnológica: importancia y riesgos en su garantía. En *Reflexiones para una Democracia de calidad en una era tecnológica* (pp. 45-70). Thomson Reuters Aranzadi.

Cetina-Presuel, R., & Martínez Sierra, J. M. (2019). Algoritmos y noticias: Redes sociales como editores y distribuidores de noticias. *Revista De Comunicación*, 18(2), 261–285. https://doi.org/10.26441/RC18.2-2019-A13

Cetina-Presuel, R. (2024a). Alertadores fiables de su codificación en la DSA a la necesidad de atender sus limitaciones. En: María Isabel Serrano Maíllo y Loreto Corredoira y Alfonso (coords.) *Democracia y desinformación: nuevas formas de polarización, discursos de odio y campañas en redes. Respuestas regulatorias de Europa y América Latina.* Dykinson, pp. 251-266.

Cetina-Presuel, R. (2024b). La gestión de riesgos sistémicos en la DSA: medidas específicas contra la desinformación. En: M. Aránzazu Moretón Toquero y Rodrigo-Cetina Presuel (Dirs.). *El nuevo reglamento de servicios digitales de la Unión Europea: Nuevo enfoque regulatorio y garantías frente a los desórdenes informativos*. Aranzadi, pp. 340.

Comisión Europea (2018). A multi-dimensional approach to disinformation: Report of the independent High-level Group on fake news and online disinformation. *Directorate-General for Communication Networks, Content and Technology*. Recuperado de: https://www.ecsite.eu/sites/default/files/amulti-dimensionalapproachtodisinformation-reportoftheindependenthighlevelgrouponfakenewsandonlinedisinformation.pdf

Corredoira, L. y Gaete, C. (21 de noviembre de 2024). Así fue la desinformación que circuló durante las elecciones en Estados Unidos. *The Conversation España*. Recuperado de: https://theconversation.com/asi-fue-la-desinformacion-que-circulo-durante-las-elecciones-en-estados-unidos-244238

Corredoira y Alfonso, L. (2024). Garantías de la libertad de expresión en redes sociales y medios. Doctrina de la Junta Electoral Central durante los comicios españoles celebrados en 2023, *Revista de Derecho Político*, número 230, págs. 209-239. https://doi.org/10.5944/rdp.120.2024.41767

Corredoira y Alfonso, L. (2023). Desinformación y otros desórdenes informativos, con especial atención a la polarización social, el discurso del odio y del negacionismo. La venganza de la posverdad. En Bel Mallén, I. (Ed.) *Recuperemos el periodismo. Ideas para regenerar la profesión periodística*. Gestión 2000. Disponible en: https://hdl.handle.net/20.500.14352/103816

European Court of Auditors (2021). Disinformation affecting the EU: tackled but not tamed. Special Report. Publications Office of the European Union, pp. 29-30. Recuperado de: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf

Fernández, C.B. (2024). España 2023 y la desinformación: amenazas y esperanzas. En: Andrés Cañizález & Mariela Torrealba (Eds.). Elecciones y desinformación. Caracas, Medianálisis-Observatorio Venezolano de Fake News. La batalla de la información, pp. 183-216. Recuperado de: https://fakenewsvenezuela.org/wp-content/uploads/2023/10/Batalla-de-la-informacion-03-oct-ISBN-FINAL-1.pdf

Fletcher, R., Cornia, A., Graves, L., & Nielsen, R. K. (2018). Measuring the reach of "fake news" and online disinformation in Europe. *Australasian Policing*, 10(2), 25-33.

Gillespie, T. (2018). Regulation of and by platforms. En Burgess, J., Marwick, A. & Poell, T. (Eds.). *The sage handbook of social media*. SAGE Publications Ltd, pp. 254-278. https://doi.org/10.4135/9781473984066

González-Urbaneja, F. (2023). Restauremos el valor de la verdad. De dónde venimos, dónde estamos y adónde vamos. En I. Bel Mallén. *Recuperemos el periodismo. Ideas para regenerar la profesión periodística.* Gestión 2000.

Iosifidis, P., & Nicoli, N. (2020). *Digital democracy, social media and disinformation*. Routledge.

Iosifidis, P. (2024). Theoretical understanding of State-Sponsored Disinformation. En Echeverría, M., García Santamaría, S. & Hallin, D. (Eds.). *State-Sponsored Disinformation Around the Globe. How Politicians Deceive their Citizens*. Routledge.

Judge, E. F., & Korhani, A. M. (2020). Disinformation, digital information equality, and electoral integrity. *Election Law Journal: Rules, Politics, and Policy*, 19(2), 240-261.

Jungherr, A., & Schroeder, R. (2021). Disinformation and the structural transformations of the public arena: Addressing the actual challenges to democracy. *Social Media+ Society*, 7(1), 2056305121988928.

Krafft, P. M., & Donovan, J. (2020). Disinformation by Design: The Use of Evidence Collages and Platform Filtering in a Media Manipulation Campaign. *Political Communication*, 37(2), 194–214. https://doi.org/10.1080/10584609.2019.1686094.

Leersen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review* 48, https://doi-org.sare.upf.edu/10.1016/j.clsr.2023.105790

López-Nieto, L. (2024). El sistema electoral y sus garantías no son el problema sino la solución. *Cuadernos de pensamiento político FAES*, (81), 5.

Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. New York: *Data & Society Research Institute*, 7-19.

McKay, S., & Tenove, C. (2021). Disinformation as a threat to deliberative democracy. *Political research quarterly*, 74(3), 703-717.

O'Connor, C., & Joffe, H. (2020). Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines. *International Journal of Qualitative Methods*, 19. https://doi.org/10.1177/1609406919899220

Reuters Institute for the Study of Journalism. (2023). *Digital News Report 2023: Spain*. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023/spain

Rubio-Núñez, R., Franco-Alvim, F. & de Andrade Monteiro, V. (2024). *Inteligencia artificial y campañas electorales algorítmicas. Disfunciones informativas y amenazas sistémicas de la nueva comunicación política*. Centro de Estudios Políticos y Constitucionales. Ministerio de la Presidencia.

Schünemann W. J. (2022). A threat to democracies? An overview of theoretical approaches and empirical measurements for studying the effects of disinformation. In Cavelty M. D., Wenger A. (Eds.), *Cyber Security Politics* (pp. 32–47). London: Routledge.

Sivalo, D. M. (2024). An analysis of the role of disinformation in elections: An exploratory study of the Centre for Innovation and Technology's project on combating electoral disinformation in the August 2023 national and December 2023 by-elections. *African Journal of Inclusive Societies*, Volume: 4, Issue: 1 / 2024.

Starr, P. (2020). The flooded zone: How we became more vulnerable to disinformation in the digital era. En Bennett W.L. & Livingston, S. (Eds.) *The disinformation age: Politics, technology and disruptive communication in the United States*, pp. 67-91.

Stowel, A. & de Meyere, J. (2023). The Digital Services Act: Transparency as an efficient tool to curb the spread of disinformation on online platforms? Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 14(1), 66.

Syrovátka, J., Hořejš, N., & Komasová, S. (2023). Towards a model that measures the impact of disinformation on elections. European View, 22(1), 119-130. https://doi.org/10.1177/17816858231162677

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* (Vol. 27, pp. 1-107). Council of Europe.

Yuskiv, B., & Karpchuk, N. (2024). Russian Federation's FIMI prior to its Intervention in Ukraine. En M. Echeverría, S. García Santamaría & D. Hallin (Eds.). *State-Sponsored Disinformation Around the Globe. How Politicians Deceive their Citizens*. Routledge.