recibido 28.03.2025 / aceptado: 16.07.2025

Análisis de la desinformación que afecta a las organizaciones. Una perspectiva comparada entre España y Portugal

Analysis of disinformation on organizations: a comparative perspective between Spain and Portugal

Sónia Gomes Gonçalves
Universidade da Madeira

Trinidad Núñez Domínguez
Universidad de Sevilla

Nuria Sánchez-Gey Valenzuela
Universidad de Sevilla

Referencia de este artículo
Gomes Gonçalves, Sónia; Núñez Domínguez, Trinidad y Sánchez-Gey Valenzuela, Nuria (2025). Análisis de la desinformación que afecta a las organizaciones. Una perspectiva comparada entre España y Portugal. *adComunica. Revista Científica de Estrategias, Tendencias e Innovación en Comunicación*, nº30. Castellón de la Plana: Departamento de Ciencias de la Comunicación de la Universitat Jaume I, 133-164. DOI: http://dx.doi.org/10.6035/adcomunica.8756.

Palabras clave

Desinformación; *fake news;* verificación da datos*;* seguridad cibernética; fraude; *deepfakes*.

Keywords

Cybersecurity; Deepfakes; Disinformation; Fact-Checking; Fake News; Fraud.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Resumen

A nivel mundial, diferentes incidentes en campañas electorales, la pandemia Covid-19 o conflictos bélicos internacionales, han favorecido el aumento del fenómeno de la desinformación, que encuentra en las redes sociales su mayor altavoz ampliado, además, por la participación ciudadana y con consecuencias negativas no solo para personas sino también para las organizaciones, ya sean empresas, marcas, instituciones u organismos. El objetivo de este trabajo es analizar la desinformación que afecta a las organizaciones, presentando una perspectiva comparada entre España y Portugal. Para ello se ha optado por una investigación de corte metodológico mixto, cuantitativo y cualitativo, aplicando como herramienta la técnica de análisis de contenido para evaluar publicaciones de dos plataformas de *fact-checking*, Maldita.es y Polígrafo. Los resultados nos permiten inferir que las organizaciones están frecuentemente expuestas a la difusión de contenidos desinformativos, con el agravante de que no resulta fácil detectar el origen de la desinformación. Las amenazas para las organizaciones pueden tener diversas formas, desde publicaciones falsas o engañosas a intentos de fraude, campañas de difamación o rumores maliciosos. Ante un escenario en el que el avance de las nuevas tecnologías derivadas de Internet y la amplia expansión de las redes sociales facilitan la propagación de desinformación, las organizaciones se ven obligadas a adoptar constantemente nuevas estrategias de relaciones públicas, para salvaguardar su reputación e imagen y necesitan estudios y herramientas que las orienten sobre ello.

Abstract

Globally, various incidents in election campaigns, the COVID-19 pandemic, or international armed conflicts, have contributed to an increase in the phenomenon of disinformation. Social media serves as its main amplifier, further expanded by citizen participation, with negative consequences not only for individuals but also for organizations, including companies, brands, institutions, and governmental bodies. The objective of this study is to analyze the disinformation that affects the organizations, offering a comparative perspective between Spain and Portugal. To this end, a mixed-methods research design was chosen, incorporating both quantitative and qualitative approaches, employing content analysis techniques to examine publications from two fact-checking platforms: Maldita.es and Polígrafo. The results allow us to infer that organizations are frequently exposed to the spread of disinformation, further complicated by the difficulty of identifying the source of disinformation. The threats to organizations can take various forms, ranging from false or misleading publications to fraud attempts, smear campaigns, or malicious rumours. In a scenario where the advancement of new technologies derived from the Internet and the widespread expansion of social media facilitate

DOI: http://dx.doi.org/10.6035/adcomunica.8756

the dissemination of disinformation, organizations are compelled to constantly adopt new public relations strategies, particularly to safeguard their reputation and image. They also require studies and tools to guide them in this regard.

Autoras

Sónia Gomes Gonçalves [sonia.goncalves@staff.uma.pt] es Profesora Invitada de la Universidade de Madeira, Portugal.

Trinidad Núñez Domínguez [mtnunez@us.es] es Profesora Titular de la Universidad de Sevilla, España.

Nuria Sánchez-Gey Valenzuela [nsanchez-gey@us.es] es Profesora de la Universidad de Sevilla, España.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

1. Introducción y estado de la cuestión

1.1 Desinformación

La difusión de información no verificada es tan remota como la existencia humana (Valero y Oliveira, 2018; Serra Cristóbal, 2023) y el recurso del uso de bulos o noticias falseadas para engañar no es algo novedoso. Esta tendencia remonta a la antigüedad clásica y está documentada en la Ilíada, uno de los poemas épicos presumiblemente escritos por Homero, que nos presenta una eficaz estrategia de desinformación, con base en un engaño, recurriendo al Caballo de Troya (Farquhar, 2005).

Uno de los históricos casos es el del «Gran Engaño de la Luna de 1835», en el que el New York Sun publicó una serie de artículos sobre el descubrimiento de vida en la luna (Allcott y Gentzkow, 2017). Existiendo otros resaltables, uno de los motivos de estudiar este fenómeno radica en que se vive una era digital donde ha aumentado exponencialmente el consumo de Internet (Eurostat, 2024) elevándose las situaciones desinformativas (Fallis, 2015; Ireton y Posetti, 2018; Román-San-Miguel et al., 2020; Reig Cruañes, 2025).

A lo largo de los años, el fenómeno de la desinformación ha ido adquiriendo más relevancia porque su aumento se ha visto propiciado por el uso creciente de las tecnologías de información y de las redes sociales (Salaverría et al., 2024). Igualmente, un recurso como la inteligencia artificial (IA) está siendo usado por la cibercriminalidad porque está al alcance del usuario común de manera gratuita e inmediata (Centro Nacional de Cibersegurança, 2023). De hecho, desde finales del siglo XX han surgido distintas campañas desinformativas a gran escala sobre temáticas muy dispares como las relacionadas con el cambio climático, las vacunas, los alimentos, el origen de la vida, la salud, las armas, los medicamentos, la cura u origen de enfermedades, la energía nuclear o el impacto de la inmigración (Valero y Oliveira, 2018; Van Bavel y Pereira, 2018).

La desinformación ha alcanzado a la publicidad. Podemos encontrar muchos ejemplos que incluyen la publicidad engañosa, tanto en los negocios como en la política, propaganda gubernamental, fotografías manipuladas, documentos falsificados y mapas falsos (Allcott y Gentzkow, 2017; Vizueta, Guamán, & Fuentes, 2020). A esto se suman otras técnicas como el *phishing*, *smishing* y *vishing* utilizadas para engañar y obtener información personal. La primera se realiza con el uso de correos electrónicos, la segunda utilizando mensajes de texto y la tercera a a través de llamadas de teléfono. Se emplea la técnica de *spoofing* para suplantar la identidad de una web, entidad o una persona y adquirir contraseñas y/o números de tarjetas de crédito (INCIBE, s.f.; 2020a). Junto a ellas se localizan los *deepfakes* o vídeos manipulados, que son una de las formas más recientes de desinformación que está afectando a personas e instituciones (Gomes Gonçalves, 2022; Vaccari et al., 2020; Castellanos-Trujillo et al., 2025).

DOI: http://dx.doi.org/10.6035/adcomunica.8756

En paralelo a estas cuestiones se observa que las campañas para las elecciones presidenciales en Estados Unidos y en Brasil, el referéndum del Brexit, la invasión de Ucrania por parte de Rusia, el conflicto entre Israel y Palestina o la pandemia de Covid-19, entre otros, han acrecentado la tendencia hacia la proliferación de contenidos desinformativos (Morejón et al., 2022).

1.1.1 Desinformación organizacional

La comunicación en la empresa tiene que estar coordinada para facilitar la concreción de los valores fundamentales que aspira transmitir, entre los que se destacan: la gestión de la marca, la imagen corporativa, la identidad organizacional, la reputación, la responsabilidad social, la cultura corporativa y la comunicación interna, así como la claridad, transparencia y credibilidad de la información (Ventura, 2001; Reyes Hidalgo, 2023). En la era de la globalización y la digitalización las empresas se han visto obligadas a integrar nuevas formas de comunicación, como las redes sociales y las plataformas digitales, para mejor interactuar tanto con su público objetivo como con sus empleados (Mattelart, 2007). Se ha creado una nueva perspectiva de la comunicación empresarial que se define por una racionalidad renovada en la que coexisten diversas lógicas. Aunque se sigue considerando la maximización del beneficio y el retorno económico para los inversores, incorpora las expectativas de otros grupos de interés como los empleados, clientes y ciudadanía de la comunidad en la que opera la empresa (Villafañe, 2009).

En este panorama, la comunicación interna y la externa asumen un papel determinante destacando la relación entre todos los colaboradores de la empresa y su público externo, especialmente los *stakeholders* (González-Fabre, 2015).

Existen diversas formas de mentira en la comunicación empresarial. La más frecuente es el fraude relacionado con productos o sus condiciones (entrega, garantía, etc.), que no coinciden con lo prometido en la publicidad. Resulta peligroso cuando una empresa mantiene cercanía al poder político que le permite trato preferencial y crear monopolios que explotan a los consumidores. Otra forma de mentira ocurre cuando las empresas se asocian a *stakeholders* por intereses económicos sin considerar las consecuencias y ocultan estas alianzas. Algunas empresas manipulan las expectativas de los consumidores con estrategias de comunicación para asegurar que un producto satisfará todas sus necesidades (ibidem).

Por otra parte, la desinformación publicitaria gana cada vez más fuerza: los anunciantes promueven la difusión de contenidos falsos y es cada vez más común la instrumentalización de estos para afectar la reputación corporativa. Sin embargo, la mala reputación de una organización puede ocurrir simplemente porque consumidores están insatisfechos con la marca o con algún aspecto del funcionamiento organizacional como atención al cliente, por ejemplo (Blikstein et al., 2018).

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Algunas marcas financian la propagación de desinformación porque los anunciantes quieren ampliar su alcance y, como tal, se sienten atraídos por páginas web e historias populares (Berthon et al., 2018). Las propias marcas se pueden convertir en víctimas, con la intención de utilizar la reputación de las marcas para sus propios propósitos retorcidos (Peterson, 2019). Incluso para desinformar, algunas empresas o marcas recurren a los *influencers* o, mejor, a los *fake influencers*, líderes de opinión que son vistos como confiables e imparciales (Frau-Meigs, 2018), lo que les permite recomendar productos y servicios en las plataformas de redes sociales y generar una adhesión que las marcas aprovechan (De Veirman et al., 2017) porque su repercusión mediática puede llegar a provocar que el anunciante posea un mayor control sobre las decisiones estratégicas, resultando un dominio complejo de fuerzas entre anunciante y agencia (Sanz-Marcos et al., 2021).

También las instituciones, públicas o privadas, se ven perjudicadas por la multiplicidad de relatos que atacan su credibilidad, distorsionan la realidad y aumentan la desconfianza, lo que altera la paz social y la convivencia pacífica de una sociedad al igual que un delito (Marchal González, 2023). Y precisamente porque la proliferación de contenidos desinformativos puede afectar a la reputación de una organización o de una marca (Borges-Tiago et al., 2020; Mills y Robson, 2019; Peterson, 2019; Xifra, 2020) algunas campañas de desinformación tienen éxito.

Son tiempos complejos para empresas y marcas. No obstante, las organizaciones están cada vez más atentas a la difusión de contenidos desinformativos y al impacto que pueden tener porque las consecuencias pueden ser negativas, sobre todo a nivel económico (Christov, 2018). Según la perspectiva relacional (Grunig y Hung-Baesecke, 2015), la naturaleza de las relaciones públicas radica en su capacidad de gestionar las relaciones entre una organización y sus públicos o *stakeholders* través de un proceso estratégicamente planificado (Alvarado y Pulido-Polo, 2018; Almiron y Xifra, 2019; Page y Parnel, 2019) capaz de situar ante la opinión pública la excelencia del comportamiento organizacional (Greenhill, 2020). La finalidad de este proceso no es otra que la de generar confianza en esos públicos.

El principal obstáculo en la búsqueda de la confianza organizacional ha sido la desinformación que representa el objetivo del primer modelo de relaciones públicas, tal y como ocurrió con el agente de prensa, el que fue el gran reto de Ivy L. Lee figura histórica que da origen al segundo modelo, el de información pública (Castillo Esparcia, 2009). Lee es pionero en la lucha contra la desinformación corporativa que inicia para gestionar la imagen de Rockefeller a raíz de la denominada Masacre de Ludlow (Burgueño, 2014).

El desarrollo sin precedentes de las tecnologías derivadas de Internet, y en especial la amplia expansión de las redes sociales, no ha hecho sino incrementar notoriamente la problemática de la desinformación (Pulido-Polo et al., 2021; Reig Cruañes, 2025). Es cada vez más común la instrumentalización de contenidos des-

DOI: http://dx.doi.org/10.6035/adcomunica.8756

informativos para afectar la reputación organizacional con diferentes intenciones, ya sean para dañar a un competidor en el mercado o valorarlo, pero puede ocurrir simplemente por consumidores insatisfechos con la marca o con algún aspecto del funcionamiento organizacional (Blikstein et al., 2018).

Desde luego, es inadmisible que las relaciones públicas recurran a estrategias de desinformación para persuadir ya que esta opción contradice todos los sus principios éticos (Castillo Esparcia, 2009). Es que la desinformación puede tener un impacto devastador y, como tal, ser un riesgo para las empresas y las marcas que se ven obligadas a gestionar mejor la crisis reputacional (Mut Camacho y Rueda Lozano, 2022).

Las organizaciones se muestran preocupadas por el daño reputacional que contenidos desinformativos representan (AON, 2017; Estudio de Comunicación y Servimedia, 2018). Los mensajes con contenidos desinformativos pueden dañar la reputación de una empresa, y no solo por motivos políticos. También pueden estar relacionados con motivaciones financieras, emocionales o ser de carácter interno, como empleados descontentes (Reid, 2017). Es importante notar que, incluso con el gran desarrollo tecnológico que existe, las organizaciones pueden convertirse en víctimas de avances digitales como los *deepfakes* y ver su reputación dañada (Gomes Gonçalves, 2022; Cruz, et al., 2021; García-Ull, 2021; Brito d'Andréa y Henn, 2021; Galston, 2020; Westerlund, 2019). Sabiendo que la reputación es un riesgo para las empresas, marcas, instituciones y otros organismos, resulta cada vez más importante la gestión de relaciones de confianza con los públicos (Xifra, 2020).

Con la masificación de la información y la amplificación de la difusión de los contenidos desinformativos, se asume que las redes sociales tienen deberes inherentes a la responsabilidad social corporativa (RSC). Sin embargo, el deber corporativo de los desarrolladores de navegadores, redes sociales y motores de búsqueda no alcanza los estándares mínimos de responsabilidad (Safieddine et al., 2016). Por lo tanto, las empresas de plataformas sociales deben asumir responsabilidades sociales que aportarán ventajas de reputación a las empresas (Liu et al., 2021). Pero los proveedores de redes sociales saben que no es muy rentable ocuparse del monitoreo, vigilancia y moderación de discursos de odio como parte de su estrategia de RSC (Doncel-Martín et al., 2023), lo que puede provocar que la desinformación reine.

Esperanzador resulta que, como la RSC también puede ser considerada como una forma de combate a la desinformación, las acciones de las empresas puedan ayudar a rehabilitar la confianza de sus usuarios y que estos, al estar más informados, no participen en cadenas desinformativas (Jeong et al., 2022).

DOI: http://dx.doi.org/10.6035/adcomunica.8756

1.2 Plataformas de *fact-checking*: una forma de lucha contra la desinformación

En los últimos tiempos se han buscado técnicas para luchar contra la desinformación por sus peligros. Son muchas y diversas las estrategias de lucha contra la desinformación, así la regulación de la difusión de contenidos falsos, la toma de consciencia sobre la importancia de la alfabetización mediática y el papel de las plataformas de *fact-checking*.

En el contexto contemporáneo de sobreabundancia informativa y proliferación de contenidos falsos, las plataformas de *fact-checking* han emergido como actores clave en la lucha contra la desinformación. Estas plataformas, dedicadas a la verificación del discurso público y de contenidos difundidos en medios y redes sociales, se han multiplicado globalmente en los últimos años buscando legitimar la verificación de datos como periodismo imparcial y establecer estándares y prácticas comunes em esta área, asegurándose una financiación fiable para este género emergente (Graves, 2016).

Uno de los hitos más significativos en la institucionalización del fact-checking ha sido la creación de la International Fact-Checking Network (IFCN) en 2015. Esta red es un referente en las mejores prácticas y el intercambio de información basada en hechos desde su fundación. Agrupa a las principales entidades de verificación del mundo y promueve un código de principios compartidos, como la imparcialidad, la transparencia y el compromiso con la corrección (IFCN, s.f.).

El combate a la difusión de contenidos desinformativos en línea ha llamado la atención sobre el potencial de varias tecnologías de *fact-checking* y se presenta como una herramienta esencial contra la desinformación (Mayoral et al., 2019).

Muchas veces la información es difundida de manera viral, sobre todo en las redes sociales sin control de su difusión, aunque el contenido sea nocivo. En este escenario, la libertad de expresión se confunde con la libre propagación de ideas (Esteves y Sampaio, 2019). Y esto puede suceder en diversos campos, desde políticos a mercadólogos, desde grupos de presión a marcas, todos los que intenten convencer con incentivo para distorsionar, exagerar u ofuscar los hechos (Ireton y Posetti, 2018).

El *fact-checking* puede definirse como una práctica periodística basada en la comprobación *a posteriori* de informaciones publicadas por los medios. Por ejemplo, se incluye la verificación de declaraciones o comentarios realizados por líderes políticos o personajes relevantes (Vázquez-Herrero et al., 2019) o en una corriente del periodismo contemporáneo (Graves y Anderson, 2020). Incluso como una herramienta de construcción de la democracia que surge cuando las instituciones democráticas se perciben débiles o amenazadas. Éstas, por tanto, examinan las similitudes entre el crecimiento de las intervenciones de verificación de datos y los movimientos de reforma del consumidor (Amazeen, 2020). Es consecuencia del aumento de la desinformación que cada vez haya más colectivos y agencias especializadas en verificación de contenidos (Graves y Cherubini, 2016; Pérez-Curiel y Velasco-Molpeceres, 2020) y, a la vez, desde el punto de vista de la estructura

DOI: http://dx.doi.org/10.6035/adcomunica.8756

de la información hay también cada vez más interés en saber quiénes están detrás de estas iniciativas de verificación (Rica y Valenzuela, 2023).

Con los avances tecnológicos y el surgimiento de nuevas herramientas como la inteligencia artificial (IA) se intenta adaptar las plataformas de *fact-checking*, algo todavía difícil porque en esta área todavía no es posible recurrir a la IA sin intervención humana, que ayude a contextualizar y traducir adecuadamente lo que se desea analizar sin el riesgo de que se genere censura previa (Larrondo y Grandi, 2021). En el *fact-checking*, aunque en España y en Portugal todavía no se utilicen, ya han surgido sofisticados programas lingüísticos que permiten analizar cuerpos y detectar contenidos desinformativos. Mecanismos automáticos, como el de *text mining* (minería de textos), son utilizados para detectar el uso o la ausencia de características lexicales, gramaticales y sintácticas, así como aspectos semánticos o retóricos (O'Brien et al., 2018; Marquardt, 2019; Mahyoob et al., 2021). Se considera oportuno el recurso a las plataformas de *fact-checking* para verificar de qué forma se difunde la desinformación organizacional en España y Portugal.

2. Objetivos

Los objetivos están precedidos por la siguiente pregunta: ¿La desinformación afecta a las organizaciones, ya sean empresas, marcas, instituciones u otros organismos? A raíz de este interrogante, se plantea como objetivo principal analizar los contenidos desinformativos que afectan a las organizaciones, reflexionando sobre la desinformación organizacional y presentando una perspectiva comparada entre España y Portugal. Como consecuencia de este objetivo principal, se definen los siguientes objetivos específicos:

- Contextualizar teóricamente los distintos aspectos relacionados con la desinformación organizacional;
- Analizar una selección de verificaciones de contenidos publicada en dos plataformas de *fact-checking*, Maldita.es y Polígrafo, con diferentes propósitos y según la muestra en estudio:
- Identificar qué tipo de publicaciones son verificadas por las dos plataformas.
- Analizar las principales formas de propagación de la desinformación.
- Constatar el origen y la posible motivación de los contenidos desinformativos.
- Comprobar que tipo de organizaciones son más afectadas con los contenidos desinformativos.
- Demostrar cuáles son las principales amenazas que pueden representar los contenidos desinformativos para las organizaciones.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

3. Metodología

En esta investigación se ha optado por una metodología mixta, cuantitativa y cualitativa. A través de la técnica de análisis de contenido y teniendo en cuenta los pasos que se deben llevar a cabo para que el proceso de análisis de datos sea exitoso (Miles y Huberman, 1994), se siguen las fases propuestas por Bardin (1977): preanálisis, exploración del material y tratamiento de los resultados obtenidos.

En la fase de preanálisis, después de una profunda revisión bibliográfica, se ha concluido que es de interés el estudio de la desinformación que afecta a las organizaciones a través del análisis de publicaciones en plataformas de verificación de contenidos de España y Portugal, lo que permite comparar la realidad de dos países. Al decidir la muestra concreta, se optó por una etapa temporal en la que ninguno de los países estuviera sujeto a un escrutinio electoral, ya que el objetivo no es realizar una valoración de la desinformación de ámbito político, no queriéndose que esa información determinara los resultados.

En la fase de preparación de material se decide seleccionar las publicaciones en el periodo temporal de tres meses, en dos plataformas de *fact-checking*: Maldita.es y Polígrafo. La elección de éstas se debe a que ambas han sido en su país las primeras *fact-checking* y se han convertido en referentes en la verificación de datos, además de que son apreciadas por el público, por su credibilidad. Se considera que el periodo de tiempo analizado (se han estudiado las informaciones durante tres meses) es representativo ya que ambas páginas web publican con regularidad, normalmente a diario, y con más de una publicación al día. Asimismo, las dos integran a reputadas organizaciones internacionales de verificación de datos, como el International Fact-Checking Network (IFCN) y el proyecto Iberian Digital Media Research and Fact-Checking Hub (IBERIFIER).

En lo que respecta a la exploración del material, los datos analizados se extrajeron de los últimos tres meses del año 2023. En un primer momento se hizo de forma automática a través del programa Octoparse (v8.6.5.91512), y después manualmente en todos los documentos que requirieron una interpretación cualitativa previa, lo que ha permitido aumentar el nivel de confianza en la muestra.

Para la extracción, se ha creado tablas en Excel con diferentes campos y se ha tenido en cuenta los siguientes ítems: frecuencia, calificación (bulo; timo; qué sabemos; sin pruebas; verdadero; impreciso; descontextualizado; manipulado; falso; verdadeiro más, pimenta na lingua), forma de difusión, origen, a quiénes afecta y tipo de contenido (instituciones; empresas; partidos políticos u otros):

En cuanto a la tercera fase, la del tratamiento de los resultados, los datos codificados en el programa Excel han sido tratados a través del software de análisis estadístico SPSS y del programa de análisis de datos Julius IA, un analista de IA que ayuda a valorar y visualizar los datos, relacionándolos. La esencial validación se

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Tabla 1. Campos utilizados para la extracción de datos.

N.º	Fecha	Fact-check	Calificación	Difusión	Fuente	Quién afecta	Tipo	Link

Fuente: Elaboración propia.

ha hecho a través de los filtros de las columnas Excel, que ha permitido confirmar o corregir los análisis y elaborar los gráficos, a través de tratamiento estadístico.

La muestra está compuesta por el total de N publicaciones extraídas de las dos plataformas de *fact-checking*. De la muestra general (N=823), se deriva una muestra específica que incluye únicamente las publicaciones desinformativas (N=631).

4. Resultados de la investigación

4.1 Análisis de las verificaciones de las plataformas Maldita.es y Poligrafo

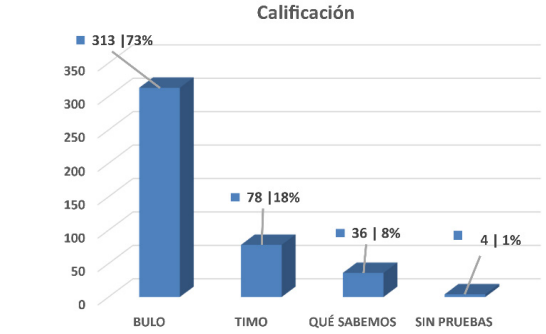
De agosto a octubre de 2023, la plataforma española de verificación de contenidos Maldita.es ha publicado un total de 431 verificaciones de contenido en las secciones Maldito Bulo y Timo. Por su parte, en las mismas fechas, el periódico portugués de *fact-checking* Polígrafo ha publicado un total de 392 verificaciones de contenido en la sección Fact-Checks.

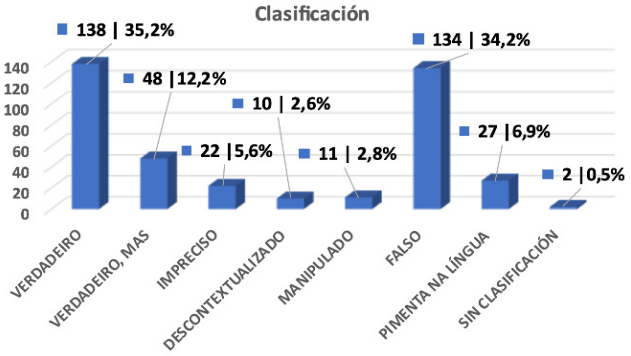
En cuanto a la calificación, en Maldita.es, una gran mayoría de las publicaciones analizadas, el 73%, ha sido calificada como «bulo», seguida de la categoría «timo» (18%). Todavía, se constata que un 8% de las verificaciones han sido catalogadas como «qué sabemos» y 1% como «sin pruebas». En Polígrafo, se destacan las publicaciones con las calificaciones de «verdadeiro» y «falso», con 35% y 34%, respectivamente. Se siguen las catalogaciones de «verdadeiro, mas» (12%), «pimenta na língua» (7%), «impreciso», «descontextualizado» y «manipulado». Del total de las verificaciones, 0,5% no han sido catalogadas.

Con respecto a la forma de difusión, es necesario destacar que en Maldita.es una mayoría considerable de las verificaciones, el 82%, se ha difundido exclusivamente a través de las redes sociales; el 19% se ha divulgado por medio de otros canales (correo electrónico, SMS, anuncios, llamadas telefónicas y medios de comunicación) y el 7% corresponden a contenidos que se han catalogado en este estudio como «no aplicable», como casi todos los de la categoría «qué sabemos». En Polígrafo, hay que enfatizar que una mayoría, el 74% de los contenidos verificados, se ha difundido exclusivamente a través de las redes sociales y un 1,5% no ha sido catalogado por referirse a otros canales de proliferación (correo electrónico, alertas de lectores y comentarios en páginas web).

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Figuras 1 y 2. Calificaciones de las verificaciones analizadas (Maldita.es y Polígrafo)





Fuente: Elaboración propia.

Sobre el origen (fuente), las publicaciones verificadas por la plataforma Maldita.es y Polígrafo son mayoritariamente (79,4% / 59%) no institucional, o sea, la desinformación posee una procedencia individual. En Polígrafo, se observa que algunos contenidos (cerca de 20%) tienen origen en eventos mediáticos, como discursos o intervenciones en reuniones plenarias, o en declaraciones realizadas a los medios de comunicación, entrevistas y reacciones a noticias.

En Maldita.es, entre los canales, páginas y cuentas troll que difunden desinformación, se destaca El Puntual 24H, cuyos tuits nunca dirigen a una página web, ni contienen ningún enlace como fuente a pesar de que van acompañados de la etiqueta #URGENTE para crear sensación de alarma y apelar a los sentimientos de las personas (Maldita.es, 2023a).

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Merecen destaque las cuentas troll que difunden contenidos desinformativos y otras cuentas falsas que tienen como principal objetivo intoxicar el debate en torno a determinados temas. Como la de Jacinta Rebolledo, que se presenta como alguien conectado al partido político Podemos, pero que en realidad no hace más que desinformar (Maldita.es, 2023a), y la cuenta de Susana Pérez (susanantonp), que se exhibe como una «profesora progresista», pero que en realidad es una cuenta falsa que se hace pasar por feminista (Maldita.es, 2023b).

Se confirma la creación de cuentas falsas con el principal objetivo de incidir sobre la clase política, concretamente sobre el presidente del Gobierno de España, Pedro Sánchez, y su vicepresidente, Yolanda Díaz.

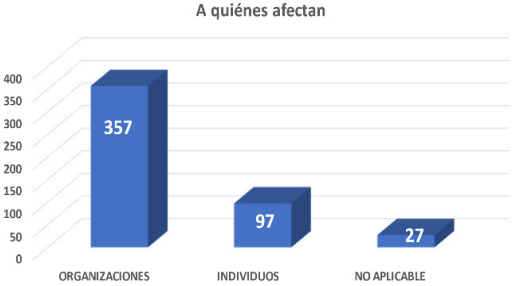
En Polígrafo, los contenidos de origen no institucional son muy variados. Cerca de 20% son sobre eventos mediáticos, como discursos o intervenciones en reuniones plenarias, así como declaraciones realizadas a los medios de comunicación, entrevistas y reacciones a noticias y, sin mucha presencia (1%), algunos de los contenidos verificados tienen origen en páginas falsas que difunden contenidos desinformativos. En estos, se comprueba que se ha usurpado la identidad de los CTT (correos), del supermercado Mercadona, de la Rádio Renascença y de la revista The Lancet, por ejemplo.

Con relación a quiénes son las víctimas de estos contenidos verificados y el tipo de contenidos es necesario precisar que se considera afectada una organización o un individuo siempre que la publicación es sobre esta/e haya generado una verificación, aunque el contenido no sea desinformativo. Se constata que un mismo contenido puede afectar, a la vez, a una o varias organizaciones, así como a organizaciones y a individuos al mismo tiempo. En las dos plataformas las publicaciones afectan predominantemente a las organizaciones. En Maldita.es, los contenidos difundidos afectan mayoritariamente a las organizaciones ya que, de un total de 431 verificaciones analizadas, 357 afectan directamente instituciones, empresas, marcas u otro tipo de organizaciones. En Polígrafo, del total de las verificaciones analizadas (392), la mayoría (334) afecta también a las organizaciones.

Los resultados del análisis permiten afirmar que, en Maldita.es, de un total de 431 publicaciones verificadas, 73% (311) afecta al menos a un tipo de organización, que puede ser empresa o marca (también personalidad), institución u organismo. En Polígrafo, de un total de 392 contenidos verificados, 85% (334) afecta a las organizaciones.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Figuras 3 y 4. A quiénes afectan los contenidos verificados por Maldita.es y Polígrafo.



Fuente: Elaboración propia.

Figuras 5 y 6. Contenidos verificados que afectan a las organizaciones (Maldita.es y Polígrafo).

Fuente: Elaboración propia.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

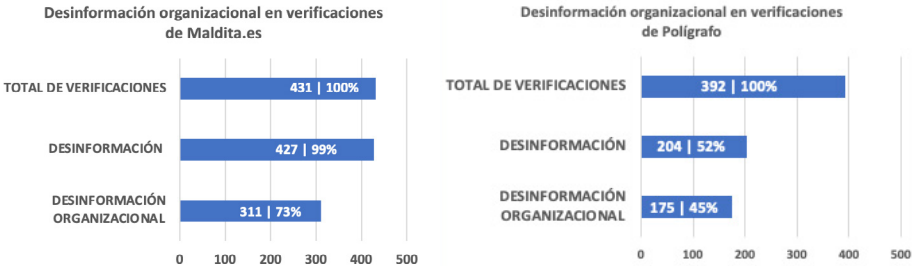
4.1.1 Desinformación organizacional en las verificaciones de Maldita.es y Polígrafo

De los datos se extrae que, en Maldita.es, casi todos los contenidos que afectan a las organizaciones son desinformativos, mientras que, en Polígrafo, sólo 45% de los contenidos que afectan a las organizaciones son desinformativos.

Como ya se ha referido, la misma verificación puede afectar, a la vez, a una o más organizaciones. Así, tanto en Maldita.es como en Polígrafo, la desinformación organizacional impacta, de forma más incisiva a las instituciones y, posteriormente, a las empresas.

Analizando la desinformación organizacional en los contenidos verificados por las dos plataformas en lo que se refiere a las instituciones, se constata que tanto en España como en Portugal el Gobierno Central es el principal objetivo, pero también hay publicaciones que involucran a instituciones de gobiernos regionales y locales, la Casa Real (España), gobiernos extranjeros y distintos organismos europeos, como la Unión Europea, la Comisión Europea y el Parlamento Europeo.

Figuras 7 y 8. Desinformación organizacional (Maldita.es y Polígrafo).

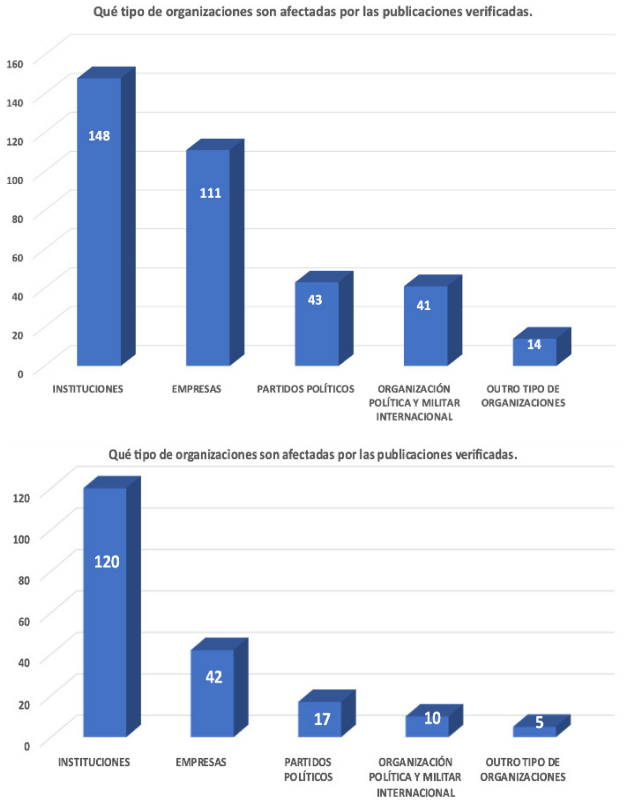


Fuente: Elaboración propia.

En cuanto a los datos extraídos, los resultados demuestran que, según el estudio de la plataforma española, la desinformación tiene mayor impacto en las empresas. Nombres de grandes marcas como Coca-Cola, Bizum, Correos, Dyson, Lidl, Leroy Merlin, McDonald's, Mercadona, Metro de Madrid, Netflix, Repsol, Renfe, Whatsapp y Women'secret aparecen en publicaciones desinformativas con el objetivo de timar. El engaño se hace a través de promociones, sorteos y oportunidades atractivas. En Portugal, el total de empresas afectadas con contenidos desinformativos es menor y se puede concluir que los ataques desinformativos son bastante más diversificados, con incidencia apenas en el Mercadona, la Rádio Renascença, los CTT (correos de Portugal) y la industria farmacéutica.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Figuras 9 y 10. Tipo de organizaciones afectadas por desinformación organizacional en las verificaciones de Maldita.es y Polígrafo.



Fuente: Elaboración propia.

En España, de todos los partidos políticos que ocurren en los contenidos desinformativos verificados, los partidos PP y VOX son los que más publicaciones han generado. En Portugal, el PS, que es el partido que detenía el poder cuando fueron verificados los contenidos, es el que acumula más publicaciones desinformativas, lee siguen los partidos CHEGA, PSD, IL y BE.

Dado que la selección de contenidos se ha hecho entre agosto y octubre, hay que indicar que en las dos plataformas se ha encontrado variadísima desinformación sobre el conflicto armado palestino-israelí que se inició el 7 de octubre de 2023.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

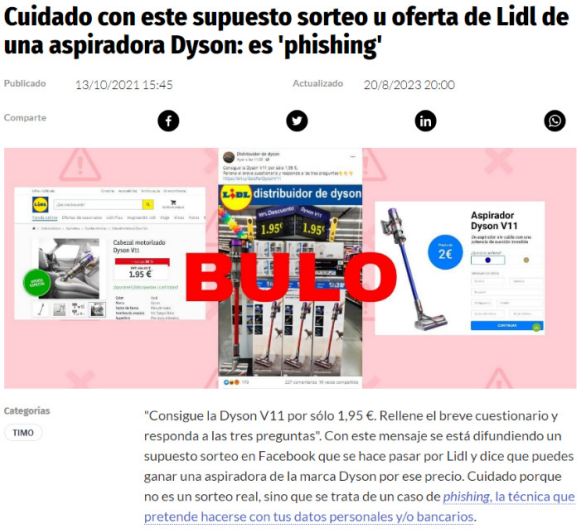
4.3 Ejemplos de desinformación organizacional

Del estudio de la muestra seleccionada, se extraen estos ejemplos de contenidos desinformativos que afectan a las organizaciones mediante el uso de técnicas de *phishing*, *smishing*, *vishing*, *spoofing* y *deepfakes*, o utilización de figuras públicas.

4.3.1 Desinformación con recurso a *phishing*

Esta técnica se utiliza para obtener información confidencial como contraseñas, números de tarjetas de crédito y otros datos personales de usuarios y para instalar programas maliciosos, *malware*, en sus dispositivos (INCIBE, 2023). El *modus operandi* es similar en casi todos los casos estudiados. Hay una supuesta ventaja, como una promoción o un sorteo, con un enlace que dirige a una página falsa o a un perfil en redes sociales que no corresponde al oficial de la empresa o marca, siendo que el principal objetivo es desinformar, engañando.

Figura 11. Desinformación con recurso a esquema de *phishing*: sorteo falso que dirige a páginas web y redes sociales no oficiales.



Fuente: Maldita.es.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

4.3.2 Desinformación con recurso a *smishing*

La técnica consiste en el envío de SMS a las víctimas haciéndose pasar por diversas entidades de confianza. El objetivo es obtener toda la información personal (usuarios y contraseñas, correos electrónicos, números de teléfono, direcciones, etc.) y bancaria para llevar a cabo nuevos fraudes o apoderarse del dinero de las víctimas (INCIBE, 2021).

Figura 12. Desinformación con recurso a smishing: alerta falsa que dirige a una página web falsa.

Fuente: Maldita.es.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

4.3.3 Desinformación con recurso a *vishing*

El *vishing* es un tipo de fraude basado en la ingeniería social y en la suplantación de identidad (*spoofing*), utilizando el teléfono. Los datos de las víctimas son obtenidos previamente a través de *phishing* y, mediante una llamada, el atacante suplanta la identidad de una organización o persona.

Figura 13. Desinformación con esquema de vishing: suplantación de identidad a través de llamada telefónica y SMS para obtener datos bancarios.

Fuente: Maldita.es.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

4.3.4 Desinformación con recurso a *spoofing*

El *spoofing* consiste en suplantar la identidad del remitente. Los ciberdelincuentes buscan engañar a la víctima para que revele información confidencial, como contraseñas, datos bancarios o credenciales de acceso. La técnica también se utiliza para suplantar páginas web, a través de la creación de otras que imitan el diseño de las originales, con URL similar. En el análisis, varios bancos y empresas de comunicación social han sido suplantados con la finalidad de engañar, concretamente el BBVA y el Sabadell y los periódicos El Mundo, Público y Tribuna Nacional; las revistas Hola, El Jueves y Time; los canales BBC, Canal 24, RTVE y RTP; y la Rádio Renascença.

Figura 14. Desinformación con recurso a spoofing: creación de una página web que imita el diseño de la página original de una marca.

Fuente: Maldita.es.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

4.3.5 Desinformación con recurso a *deepfake*

El *deepfake* permite manipular vídeos y voces mediante el uso de inteligencia artificial. En el ejemplo seleccionado, un vídeo que fue ampliamente difundido en las redes sociales muestra a la presentadora Beatriz Pérez-Aranda del Canal 24h de TVE anunciando un supuesto nuevo método infalible de inversión, el Bitcoin Millonario, que es explicado en una supuesta conferencia con el conocido empresario y emprendedor Elon Musk, CEO de la empresa Tesla.

Figura 15. Desinformación utilizando *deepfakes*: vídeos y voces manipuladas.

Fuente: Maldita.es.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

4.3.6 Desinformación utilizando figuras públicas

En algunos contenidos desinformativos se utilizan figuras públicas para lograr un mayor impacto. En la muestra, para incidir sobre determinadas organizaciones, se constata la utilización de fotos descontextualizadas y declaraciones falsas de figuras públicas, así como, por ejemplo, la publicación en las redes sociales de falsas muertes de personalidades. En las publicaciones analizadas, Cristiano Ronaldo, David Bisbal, Santiago Segura, Jaime Lorante, José Luís Perales, Rosa Montero, Elon Musk, Pedro Cavadas, Isabel Balado y Ana Belén aparecen asociados a variadísimos contenidos desinformativos que pueden dañar su reputación organizacional.

Figura 16. Desinformación utilizando una figura pública: suplantación de identidad de una editorial y publicación en redes sociales sobre la falsa muerte de un escritor.

Fuente: Maldita.es.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

4.3.7 Desinformación publicitaria

Para conseguir mayor alcance de los contenidos desinformativos, se utiliza el recurso de la publicidad, utilizando anuncios en las redes sociales, en plataformas digitales de reserva de alojamiento y en motores de búsqueda en línea. Los contenidos falsos van desde supuestas oportunidades para alquilar casa a través de Booking a regalos de maletas Samsonite, pero también super descuentos en páginas suplantadas de Women'secret y Temu. Incluso, con la finalidad de obtener, de forma fraudulenta, datos de los utilizadores se ha publicitado en las redes sociales anuncios de un falso programa del Gobierno para instalar placas solares.

Figura 17. Desinformación publicitaria difundida a través de anuncio en la plataforma de reservas de alojamiento en línea Booking.

Fuente: Maldita.es.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

5. Conclusiones

El objetivo general que se ha planteado en este trabajo ha sido analizar los contenidos desinformativos que afectan a las organizaciones, reflexionando sobre la desinformación organizacional y presentando una perspectiva comparada entre España y Portugal. Para lograr su consecución, tras construir un marco teórico gracias a una extensa revisión de la literatura emergente, se ha procedido al análisis de una selección de las verificaciones publicadas en dos plataformas de *fact-checkings*.

El cumplimiento del objetivo general se ha materializado en lo siguiente descrito. Durante la investigación se han contextualizado teóricamente los distintos aspectos relacionados con el objeto de estudio, evidenciando que el avance de las tecnologías derivadas de Internet y la amplia expansión de las redes sociales hacen que la propagación de contenidos desinformativos sea cada vez más sencilla, lo que genera un notable aumento de riesgos para empresas, marcas, instituciones y otros organismos, que se ven obligados a adoptar constantemente nuevas estrategias en términos de relaciones públicas, especialmente en lo que respecta a la reputación organizacional y la imagen de marca. Se destaca la importancia de las plataformas de *fact-checking* como una forma de combatir la desinformación, evidenciando que, para una eficaz utilización de la inteligencia artificial en los *fact-checkers*, lo ideal sería que dichos avances de la tecnología vayan de la mano de la intervención humana.

Con respecto a la muestra, el análisis de contenido permite concluir que una gran mayoría de las verificaciones de Maldita.es y de Polígrafo se refiere a contenidos desinformativos que perjudican a una o más organizaciones, ya sea una empresa, una marca, una institución u otro organismo. Las organizaciones perjudicadas son, en la mayoría de las ocasiones, un blanco fácil para quien desee difundir contenidos desinformativos, con la agravante de que no siempre es posible detectar el origen de la desinformación, pues la difusión hace que se pierda el rastro de la procedencia y, muchas veces, la desinformación en las redes sociales parte de perfiles falsos.

Importa destacar que la desinformación es propagada esencialmente a través de las redes sociales y tiene origen no institucional; o sea, posee una procedencia individual. Pero también se verifican otras fuentes: canales y cuentas troll desinformativos, publicaciones falsas en los medios de comunicación social suplantados a través de montajes, páginas web falsas y anuncios publicitarios falsos, así como declaraciones realizadas a los medios de comunicación, entrevistas y reacciones a noticias – estas predominan en la plataforma portuguesa porque esta no solo verifica contenidos desinformativos que suelen circular en las redes sociales sino también información difundida por los medios de comunicación. A pesar de estas diferencias, la motivación es común: engañar el destinatario, muchas veces con la intención de difamar a una organización y otras de obtener datos personales y bancarios para defraudar a los usuarios.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Finalmente, se constata que la desinformación afecta de forma evidente a las instituciones, los siguientes en la escala de perjudicados son las empresas, los partidos políticos, las organizaciones políticas y militares internacionales y otro tipo de organizaciones, como las deportivas, religiosas y sin fines de lucro. Los ataques desinformativos pueden adoptar diversas formas, como falsas publicaciones engañosas, intentos de fraude, campañas de difamación que pretenden dañar la reputación de una empresa o marca, rumores maliciosos, o publicaciones falsas que pretenden engañar sin ningún propósito más que el entretenimiento. Por otra parte, todas representan serias amenazas para las organizaciones, porque ponen en causa su imagen y consecuentemente su reputación como por los efectos que pueden tener a varios niveles, pues afectan la percepción pública y la confianza en estas. Además, pueden tener repercusiones económicas significativas como la pérdida de clientes, ingresos y oportunidades de negocio.

Como se ha expuesto en el estado de la cuestión, ante este escenario en el que la desinformación (originada por intereses externos o internos) puede representar un enorme riesgo para las organizaciones, dañando su reputación. Por ese motivo, se convierte en relevante que éstas adopten constantemente nuevas estrategias de relaciones públicas que les permitan consolidar la confianza de los públicos y asuman actitudes de responsabilidad social que salvaguarden su imagen.

La principal limitación encontrada ha sido la escasa bibliografía específica: la desinformación organizacional está insuficientemente explorada. En el desarrollo del procedimiento, se han encontrado limitaciones relacionadas con el tamaño de la muestra y con la extracción. Con respecto al tamaño de la muestra, naturalmente aumentarla implicaría obtener unos resultados más reveladores, si cabe. Por su parte, ampliar el periodo temporal e incluir otras plataformas dotaría de mayor capacidad para generalizar los resultados.

El hecho de que se haya llevado a cabo la extracción de datos de las plataformas de *fact-checking* de forma manual ha conllevado una dificultad añadida y un trabajo manual bastante laborioso para evitar fallos de tipo humano como, por ejemplo, la inclusión de erratas de digitación simples o el intercambio de filas en Excel. Es por ello que ha sido preciso redoblar la atención. Cierto es que, aunque esta limitación técnica inicial pudiera ser valorada como algo negativo, finalmente ha posibilitado un efecto secundario positivo porque ha permitido aumentar el nivel de confianza sobre los datos aportados.

Para dar continuidad a este proyecto sería valorable el uso de herramientas de inteligencia artificial que permitan la detección automática de contenidos desinformativos (publicitarios o no) publicados en las redes sociales y en los buscadores, que afectasen a las organizaciones. Con esto se podría ampliar la muestra y corroborar que se siguen cumpliendo los resultados obtenidos.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Referencias

Allcott, Hunt y Gentzkow, Matthew (2017). Social Media and Fake News in the 2016 Election. En: *Journal of Economic Perspectives*, Vol.31, nº2, 211–236. DOI: http://doi.org/10.1257/jep.31.2.211

Almiron, Núria y Xifra, Jordi (Eds.). (2019). *Climate change denial and public relations: strategic communication and interest groups in climate inaction*. Londres: Routledge. DOI: https://doi.org/10.4324/9781351121798

Amazeen, Michelle A. (2020). Journalistic interventions: The structural factors affecting the global emergence of fact-checking. En: *Journalism*, Vol.21, nº1, 95-111. DOI: https://doi.org/10.1177/1464884917730217

AON (2017). *Global Risk Management Survey.* Consultado el 20 de enero de 2024 en https://tinyurl.com/3ca7hd9b

Alvarado, María Teresa Otero y Pulido-Polo, Marta (2018). *Planificación y técnicas de relaciones públicas*. Madrid: Síntesis.

Bardin, Laurence (1977). *Análise de conteúdo*. Lisboa: Edições 70.

Berthon, Pierre, Treen, Emily y Pitt, Leyland (2018). How truthiness, fake news and post-fact endanger brands and what to do about it. En: *NIM Marketing Intelligence Review*, nº10, 18-23. DOI: https://doi.org/10.2478/gfkmir-2018-0003

Blikstein, Isidro; Fernandes, Manoel y Coutinho, Marcelo (2018). Fake news no mundo corporativo. En: *GV-EXECUTIVO*, Vol.17, nº5, 22-25.

Borges-Tiago, Teresa; Tiago, Flavio; Silva, Osvaldo; Guaita Martínez, José Manuel y Botella-Carrubi, Dolores (2020). Online users' attitudes toward fake news: Implications for brand management. En: *Psychology y Marketing*, Vol.37, nº9, 1171–1184. DOI: https://doi.org/10.1002/mar.21349

Brito d'Andréa de, Carlos Frederico; y Henn, Ronaldo (2021). Desinformação, plataformas, pandemia: um panorama e novos desafios de pesquisa. En: *Fronteiras-estudos midiáticos*, Vol.23, nº2. DOI: https://doi.org/10.4013/fem.2021.232.01

Burgueño, José Manuel (2014). *Comunicación institucional para periodistas. Manual práctico de comunicación y relaciones públicas*. Barcelona: UOC.

Castellanos-Trujillo, Vianny y Rodríguez-Ferrándiz, Raúl (2025). Publicidad programática y desinformación en España. El rol de marcas y plataformas AdTech en pseudomedios. En: *Revista Mediterránea de Comunicación*, Vol.16, nº2, e29240. DOI:

https://doi.org/10.14198/MEDCOM.29240

Castillo Esparcia, Antonio (2009). *Relaciones Públicas. Teoría e Historia*. Barcelona: UOC.

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Christov, Alexander (2018). Economics Effects of the Fake news on Companies and The Need of New PR Strategies. En: *Journal of Sustainable Development*, Vol. 8, nº20, 41-49.

Cruz, Ederval Pablo Ferreir da; Pereira, Rodolfo Moura; Jubini, Gilberto Mazoco; Quarto, Lucas Capita y de Souza, Carlos Henrique Medeiros (2021). Fake news: uma revisão compreensiva e interdisciplinar. En: *Cadernos de Educação Tecnologia e Sociedade*, Vol.14, nº3, 502-520. DOI: https://doi.org/10.14571/brajets.v14.n3.502-520

De Veirman, Marijke; Cauberghe, Veroline y Hudders, Liselot (2017). Marketing through Instagram influencers: The impact of number of followers and product divergence on brand attitude. En: *International Journal of Advertising*, Vol.36, nº5, 798–828. DOI: https://doi.org/10.1080/02650487.2017.1348035

Doncel-Martín, Israel; Catalan-Matamoros, Daniel y Elías, Carlos (2023). Corporate social responsibility and public diplomacy as formulas to reduce hate speech on social media in the fake news era. En: *Corporate Communications: An International Journal*, Vol.28,nº2, 340-352. DOI: https://doi.org/10.1108/CCIJ-04-2022-0040

Esteves, Fernando y Sampaio, Gustavo (2019). *Viral: a epidemia de fake news e a guerra da desinformação*. Porto Salvo: Desassossego.

Estudio de comunicación (2018). Influencia de las noticias falsas en la opinión pública. Consultado el 20 de Octubre de 2023 en https://tinyurl.com/j2adumx3

Eurostat (2024). Internet use by individuals, 2013 - 2024. Consultado el 10 de febrero de 2025 en https://doi.org/10.2908/TIN00028

Fallis, Don (2015). What Is Disinformation? En: *Library Trends*, Vol.63, nº3, 401-426. DOI: https://doi.org/10.1353/lib.2015.0014

Farquhar, Michael (2005). *A Treasury of Deception: Liars, Misleaders, Hoodwinkers, and the Extraordinary True Stories of History's Greatest Hoaxes, Fakes, and Frauds*. Londres: Penguin.

Frau-Meigs, Divina (2018). Societal costs of "fake news" in the Digital Single Market. European Parliament. Consultado el 16 de julio de 2025 en http://www.europarl.europa.eu/supporting-analyses

Galston, William A. (2020). Is seeing still believing? The Deepfake Challenge to Truth in Politics. Brookings, 8 de enero. Consultado el 20 de enero de 2024 en https://shorturl.at/kvGVY

García-Ull, Francisco José (2021). *Deepfakes*: el próximo reto en la detección de noticias falsas. En: *Anàlisi: Quaderns de comunicació i cultura*, nº64, 103-120. DOI: https://doi.org/10.5565/rev/analisi.3378

Gomes-Gonçalves, Sónia (2022). Deepfakes: a new form of corporate disinformation. En: *IROCAMM – International Review Of Communication And Marketing Mix*, Vol.5, nº2), 22-38. DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02

DOI: http://dx.doi.org/10.6035/adcomunica.8756

González-Fabre, Raúl (2015). Verdad y comunicación (empresarial). En Benavides, Juan, y Monfort de Bedoya, Abel. En: *Comunicación y empresa responsable*. Pamplona: EUNSA.

Graves, L. (2016). *Deciding What's True: The Rise of Political Fact-Checking in American Journalism*. Columbia: Columbia University Press.

Graves, Lucas; y Anderson, Christopher (2020). Discipline and promote: Building infrastructure and managing algorithms in a "structured journalism" project by professional fact-checking groups. En: *New Media & Society*, Vol.22, nº2, 342-360. DOI: https://doi.org/10.1177/1461444819856916

Greenhill, Brian (2020). How can international organizations shape public opinion? Analysis of a pair of survey-based experiments. En: *The Review of International Organizations*, nº15, 165-188. DOI: https://www.doi.org/10.1007/s11558-018-9325-4

Grunig, James E. y Hung-Baesecke, Chun-ju Flora (2015). The effect of relationships on public reputation and reputation on relationships: a cognitive, behavioral study. En: Ki, Eyun-Jung; Kim, Jeong-Nam y Ledingham, John A. (Eds.). *Public relations as relationship management*. Nueva York: Routledge.

IFCN (s.f.). The commitments of the Code of Principles. Consultado el 05 de julio de 2025 en https://ifcncodeofprinciples.poynter.org/the-commitments

INCIBE (s.f.). Phishing, smishing y vishing. Consultado el 05 de julio de 2025 en https://www.incibe.es/node/53390

INCIBE (2020a). ¿Qué es y cómo funciona el spoofing? Instituto Nacional de Ciberseguridad de España. Consultado el 12 de noviembre de 2023 en https://tinyurl.com/yccnrput

Ireton, Cherilyn y Posetti, Julie (2018). *Journalism, 'Fake news' and Disinformation-A Handbook for journalism Education and Training*. France. UNESCO. Consultado el 16 de julio de 2025 en https://tinyurl.com/mp2ejbem

Jeong, Myeongki; Kim, Doehum; Park, Hyumho; Zo, Hang Jung; y Ciganek, Andrew P. (2022). Corporate Social Responsibility's Influence on Misinformation in Online Platforms. En: *SSRN Electronic Journal*. 10. 2139. http://dx.doi.org/10.2139/ssrn.4096599

Larrondo, Manuel Ernesto y Grandi, Nicolas Mario (2021). Inteligencia Artificial, algoritmos y libertad de expresión. En: *Universitas-XXI, Revista de Ciencias Sociales y Humanas*, nº34, 177-194. DOI: https://doi.org/10.17163/uni.n34.2021.08

Liu, Wenjun; Wang, Chenye; Ding, Lin y Wang, Cuibo (2021). Research on the Influence Mechanism of Platform Corporate Social Responsibility on Customer

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Extra-Role Behavior. En: *Discrete Dynamics in Nature and Society*, DOI: https://doi.org/10.1155/2021/1895598

Mahyoob, Mohammad; Algaraady, Jeehaan y Alrahaili, Musaad (2021). Linguistic-Based Detection of Fake News in Social Media. En: *International Journal of English Linguistics*, Vol.11, nº1, 9-109. DOI: https://doi.org/10.5539/ijel.v11n1p99

Maldita.es (2023a). 57 bulos y desinformaciones de la cuenta de Twitter 'El Puntual 24H'. Consultado el 12 de noviembre de 2023 en https://tinyurl.com/2v4av2xa

Maldita.es (2023b). Cuidado con la cuenta de Twitter 'susanantonp', supuesta "profesora progresista de lengua": es una cuenta trol. Consultado el 12 de noviembre de 2023 en https://tinyurl.com/f4hf33rn

Marchal González, Adrián Nicolás (2023). La necesidad de un nuevo tipo delictivo: La desinformación como una amenaza para el orden público. En: *Boletín Criminológico*, Vol.29, nº219. DOI: https://doi.org/10.24310/Boletin-criminologico.2023.vi29

Marquardt, Dorota (2019). Linguistic Indicators in the Identification of Fake News. En: *Mediatization Studies*, nº3, 2-20. DOI:http://dx.doi.org/10.17951/ms.2019.3.95-114

Mattelart, Armand (2007). *Historia de la sociedad de la información*. Barcelona: Paidós Ibérica, S.A.

Mayoral, Javier; Parratt, Sonia y Morata, Monserrat (2019). Desinformación, manipulación y credibilidad periodísticas: una perspectiva histórica. En: *Historia y comunicación social*, Vol.24, nº2, 395-409. DOI:https://dx.doi.org/10.5209/hics.66267

Miles, Matthew B. y Huberman, A. Michael (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. Beverly Hills: Sage Publications.

Mills, Adam J. y Robson, Karen (2019). Brand management in the era of fake news: Narrative response as a strategy to insulate brand value. En: *Journal of Product & Brand Management*, Vol.29, nº2, 159–167. DOI: https://doi.org/10.1108/JPBM-12-2018-2150

Morejón Llamas, Noemí; Sánchez-Gey Valenzuela, Nuria y Micaletto Belda, Juan Pablo (2022). Desinformación y verificación durante los tres estados de alarma en España: el caso de Maldita Migración. En S. Olivero Guidobono, *El camino hacia las sociedades inclusivas*. Madrid: Dykinson.

Mut Camacho, Magdalena y Rueda Lozano, Antonio (2022). Las empresas ante la desinformación. La necesidad de un nuevo enfoque metodológico. En: *Vivat Academia. Revista de Comunicación*, nº155, 113-129. DOI: http://doi.org/10.15178/va.2022.155.e1327

O'Brien, Nicole; Latessa, Sophia; Evangelopoulos, Georgios y Boix, Xavier (2018). The Language of Fake News: Opening the Black-Box of Deep Learning Based De-

DOI: http://dx.doi.org/10.6035/adcomunica.8756

tectors. En: *32nd Conference on Neural Information Processing Systems (NIPS 2018)*, Montréal: CBMM Publications.

Page, Janis Teruggi y Parnell, Lawrence J. (2019). *Introduction to Strategic Public Relations: digital, global and socially responsible communication*. Nueva York: Sage.

Pérez-Curiel, Concha y Velasco-Molpeceres, Ana María (2020). Tendencia y narrativas de fact-checking en Twitter. Códigos de verificación y fake news en los disturbios del Procés (14-O). En: *adComunica*, nº20, 95-122. DOI: http://dx.doi.org/10.6035/2174-0992.2020.20.5

Peterson, Mark (2019). A high-speed world with fake news: Brand managers take warning. En: *Journal of Product y Brand Management*, Vol.29, nº2, 234–245. DOI: https://doi.org/10.1108/JPBM-12-2018-2163

Pulido-Polo, Marta; Hernández-Santaolalla, Víctor y Lozano-González, Ana-Alicia (2021). Uso institucional de Twitter para combatir la infodemia causada por la crisis sanitaria de la Covid-19. En: *Profesional de la información*, Vol.30, nº1. DOI: https://doi.org/10.3145/epi.2021.ene.19

Reid, Aaron (2017). What's the damage? Measuring the impact of fake news on corporate reputation can act as a guide for companies to navigate a post-truth landscape. En: *Communication Director*. Consultado el 16 de julio de 2025 en https://tinyurl.com/2bmwjmuj

Reig Cruañes, Pep (2025). *En manos de la desinformación*. España: Ediciones de la Universidad de Castilla-La Mancha

Reyes Hidalgo, Cristhian (2023). Reputación organizacional y redes sociales. Un análisis de los desafíos y estrategias. En: *Hologramática*, Vol.39, nº1, 73-86

Rica, María Luisa Cárdenas y Valenzuela, Nuria Sánchez-Gey (2023). Las iniciativas Fact Checking en España desde la estructura de la información. En: Julieti Sussi de Oliveira, Daniel Moya López, Bianca Sánchez-Gutierrez (coords.) *Tendencias en investigación crítica en comunicación: Comprender el poder en los medios hoy*. España: Fragua

Rodríguez-Fernández, Leticia (2019). Desinformación y comunicación organizacional: estudio sobre el impacto de las 'fake news'. En: *Revista Latina de Comunicación Social*, nº74, 1714-1728. DOI: https://doi.org/10.4185/RLCS-2019-1406

Román San Miguel, Aránzazu; Sánchez-Gey Valenzuela, Nuria y Elías Zambrano, Rodrigo. (2022). Los profesionales de la información y las fake news durante la pandemia del Covid-19. En: *Vivat Academia. Revista de Comunicación, nº*155, 131-149. DOI: http://doi.org/10.15178/va.2022.155.e1312

Román-San-Miguel, Aránzazu; Nuria Sánchez-Gey-Valenzuela y Rodrigo Elías-Zambrano (2020). Las *fake news* durante el Estado de Alarma por COVID-19. Análisis desde el punto de vista político en la prensa española. En: *Revista latina*

DOI: http://dx.doi.org/10.6035/adcomunica.8756

de comunicación social, nº78, 359-391. DOI: https://www.doi.org/10.4185/RLCS-2020-1481

Safieddine, Fadi; Masri, Wassim y Pourghomi, Pardis (2016). Corporate Responsibility in Combating Online Misinformation. En: *International Journal of Advanced Computer Science and Applications*, nº7. DOI: https://www.doi.org/10.14569/IJACSA.2016.070217

Salaverría, Ramón; Bachmann, Ingrid y Magallón Rosa, Raúl (2024). Desinformación y confianza en los medios. *Index Comunicación*, Vol.14, nº2. DOI: https://doi.org/10.62008/ixc/14/02

Sanz-Marcos, Paloma; Jiménez-Marín, Gloria y Elías Zambrano, Rodrigo (2021). Aplicación y uso del Modelo de Resonancia o Customer-Based Brand Equity (CBBE). Estudio de la lealtad de marca a través de la figura del influencer. En: *Methaodos. Revista de Ciencias Sociales*, Vol.9, nº2, 200-218. DOI: http://dx.doi.org/10.17502/mrcs.v9i2.471

Serra Cristóbal, Rosario (2023). Noticias falsas (fake news) y derecho a recibir información veraz. Dónde se fundamenta la posibilidad de controlar la desinformación y cómo hacerlo. En: *Revista de Derecho Político*, nº116, 13–46. DOI: https://doi.org/10.5944/rdp.116.2023.37147

Shell, Adam (1992). *Small Investors Return to the Street*. En: *The Public Relations Journal*., Vol.48, nº2.

Vaccari, Cristian y Chadwick, Andrew (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. En: *Social Media• Society*, Vol.6, nº1. DOI: http://doi.org/10.1177/2056305120903408

Valero, Pablo Parra y Oliveira, Lídia (2018). Fake news: una revisión sistemática de la literatura. En: *Observatorio (OBS*)*, Vol.12, nº5. DOI: https://doi.org/10.15847/obsOBS12520181374

Van Bavel, Jay J. y Pereira, Andrea (2018). The Partisan Brain: An Identity-Based Model of Political Belief. En: *Trends in Cognitive Sciences*, Vol.22, nº3, 213–224. DOI:https://doi.org/10.1016/j.tics.2018.01.004

Van Bavel, René; y Gaskell, George (2004). Narrative and systemic modes of economic thinking. En: *Culture & Psychology*, Vol.10, nº, 417-439. DOI:https://doi.org/10.1177/1354067X04042892

Vázquez-Herrero, Jorge; Vizoso, Ángel y López-García, Xosé (2019). Innovación tecnológica y comunicativa para combatir la desinformación: 135 experiencias para un cambio de rumbo. En: *Profesional de la información*, Vol.28, nº3. DOI: https://doi.org/10.3145/epi.2019.may.01

DOI: http://dx.doi.org/10.6035/adcomunica.8756

Ventura, Jordi (2001). Comunicación corporativa. En: Benavides, Juan (2001). *Dirección de comunicación empresarial e institucional*. Barcelona: Gestión 2000.

Villafañe, Justo (2009). La comunicación intangible: Reinventar la comunicación empresarial. En: Ramos-Serrano, Maria; Lora, Manuel Garrido y Rodríguez Centeno, Juan Carlos (Coords.). *Publicidad y comunicación corporativa en la era digital*. Madrid: Pirámide.

Vizueta, Alberto, Guamán, Ruth y Fuentes, Mónica (2020). Análisis de la publicidad engañosa en medio de comunicación digitales. En: *Revista Observatorio de la Economía Latioamericana*, Vol.18, nº1, 1-6.

Westerlund, Mika (2019). The emergence of deepfake technology: A review. En: *Technology Innovation Management Review*, Vol.9, nº11, 40-53. DOI: http://doi.org/10.22215/timreview/1282

Xifra, Jordi (2020). Comunicación corporativa, relaciones públicas y gestión del riesgo reputacional en tiempos del Covid-19. En: *Profesional de la información*, Vol.29, nº2, e290220. DOI: https://doi.org/10.3145/epi.2020.mar.20

DOI: http://dx.doi.org/10.6035/adcomunica.8756