IROCAMM.

INTERNATIONAL REVIEW OF COMMUNICATION AND MARKETING MIX

the mainstream review on communication

VOL. 5, N. 2
institucional.us.es/irocamm
https://revistascientificas.us.es/index.php/IROCAMM

VOL. 5

N. 2

Editorial Universidad de Sevilla

Editorial Universidad de Sevilla

FOUNDER
Gloria Jiménez-Marín

PUBLISHERS
University of Seville

PUBLISHING LOCATION
Seville – Spain

E-MAIL AND WEBSITE
irocamm@us.es / gloria_jimenez@us.es
https://revistascientificas.us.es/index.php/IROCAMM
https://editorial.us.es/es/revistas/irocamm-international-review-communication-and-marketing-mix

ORIGINAL DESIGN
www.lahuertaagencia.com

LAYOUT - TYPESETTING
Mayte Álvarez (Referencias Cruzadas)

ISSN
2605-0447

DOI
https://dx.doi.org/10.12795/IROCAMM

FOCUS AND SCOPE

IROCAMM (International Review Of Communication And Marketing Mix) publishes peer-reviewed scientific articles, reviews and essays related to commercial, persuasive, journalistic or audiovisual communication with special interest and priority in researching the communication and marketing mix, especially the intersection of both: advertising, public relations, media, consumption, commercial communication, commercial distribution, strategy... Reports, studies and experiences in these same fields are also accepted.

Texts with interdisciplinary, original approaches and innovative contributions that rigorously use the methodology of the field are especially welcome. The journal is published in open access, is multilingual and reflects future trends affecting communication.

It is aimed at academic researchers, whether consolidated or in training, who wish to disseminate the results of their research through scientific publication. It aims to provide a service to the international scientific community by fostering a space for exchange where academic scientific production derived from research applied to social communication can be shared, promoted and disseminated.

There is no charge to authors for processing or publishing an article.

BLIND PEER REVIEW

The papers included in the publication are reviewed and assessed by two experts, but in no case belonging to the same university or research centre as the author of the submitted paper. The review is carried out by the blind and anonymous reading system, so that the assessors and those assessed do not know each other's identity. The experts, using the questionnaire provided by the journal, consider whether or not the work is publishable and, in the first case, whether any modifications are advisable. In the event of a contradictory opinion among the experts, a third party is called in. In the case of texts that are rejected or subject to modifications, the author receives a corresponding explanatory note.

PUBLICATION FREQUENCY

IROCAMM - Intenational Review Of Communication And Marketing Mix is a biannual academic journal published in digital format. Since 2019 it publishes issues in the months of January and July each year.
Average time for the review process: 30 days. And, in any case, the evaluation periods shall not exceed 6 months.
Once accepted, the text is published in the section IN EDITION waiting for the closing of the issue.

INDEXING

EVALUATION SYSTEMS: Latindex (Directory, Catalogue v. 2.0 38/38 criteria, and journals online), Dialnet Métricas (C3), MIAR (ICDS = 3.5), ERIHPLUS, Dulcinea, REDIB, Academic Resources Index, Cite Factor (3.7).
DATABASES:DOAJ, Google Scholar, DRJI.
DIFUSION PORTALS:Dialnet, WorldCat, BASE, CRUE.
PLATFORMS AND METADATA: PlatCom, Crossref.

CONTACT ADDRESS

Faculty of Communication (University of Seville). B2 Office. N/n Americo Vespucio, 27, 41092. SPAIN.

IROCAMM.
INTERNATIONAL REVIEW OF COMMUNICATION AND MARKETING MIX

Editorial Universidad de Sevilla

SCIENTIFIC COMMITTEE

5

IROCAMM
International Review Of Communication And Marketing Mix

2022 YEAR
Vol. 5(2)
Biannual journal
Published in Seville (Spain) by EUS
(Editorial Universidad de Sevilla)
ISSN: 2605-0447

INDEX

IROCAMM, V. 5, N. 2 (July - December 2022)

MONOGRAPHIC SECTION:
False news and its impact on the consumption of products and brands

Guest editors:
Ph.D. Mirian Tavares (Universidade do Algarve, Portugal)
Ph.D. Pedro A. Correia (Universidade da Madeira, Portugal)
Ph.D. Nuria Sánchez-Gey Valenzuela (Universidad Pablo de Olavide, Spain)

MISCELLANEOUS SECTION

IROCAMM.
INTERNATIONAL REVIEW OF COMMUNICATION AND MARKETING MIX

Los *deepfakes* como una nueva forma de desinformación corporativa – una revisión de la literatura

Deepfakes as a new form of corporate disinformation – a literature review

Sónia Gomes-Gonçalves
Governo Regional da Madeira. Portugal.
soniaggoncalves17@gmail.com
0000-0002-5579-7761

Resumen
Los *deepfakes* son un fenómeno reciente que ha despertado especial atención e interés, no solo en el ámbito audiovisual, electoral, periodístico, publicitario o corporativo, sino también en el de la investigación científica y difusión divulgativa.
En un momento en que somos cada vez más conscientes del fenómeno de la desinformación, algunos estudiosos alertan de los impactos que esta nueva forma de *fake news* tiene en las empresas, las organizaciones y las marcas. Una breve revisión de literatura con base en bibliografía emergente publicada en español y en portugués nos permite concluir que la temática en estudio aún está poco explorada, sobre todo cuando comparada con las publicaciones a nivel internacional. Aunque existe consciencia acerca de los riesgos que el uso de esta nueva tecnología puede causar a nivel corporativo, así como sobre las amenazas que puede representar a varios niveles, también es cierto que cada vez se viene profundizando más en esta temática. Este artículo plantea una revisión de la literatura del concepto, en aras de generar un término específico con su correspondiente definición y su contexto.

Palabras clave
Deepfakes; cheap fakes; fake news; desinformación corporativa.

IROCAMM
VOL. 5, N. 2 - Year 2022
Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

Abstract
Deepfakes are a recent phenomenon that has attracted special attention and interest, not only in the audiovisual, electoral, journalistic, advertising, or corporate spheres, but also in scientific research and informative dissemination.
At a time when we are increasingly aware of the phenomenon of disinformation, some scholars warn of the impact that this new form of fake news has on companies, organisations, and brands.
A brief literature review based on emerging literature published in Spanish and Portuguese allows us to conclude that the topic under study is still under-explored, especially when compared to international publications. Although there is awareness of the risks that the use of this new technology can cause at the corporate level, as well as the threats that it can represent at various levels, it is also true that more and more research is being done on this topic. This article proposes a literature review of the concept in order to generate a specific term with its corresponding definition and context.

Keywords
Deepfakes; cheap fakes; fake news; corporate disinformation.

1. Introducción

La desinformación enfrenta un nuevo desafío. Los *deepfakes*, una nueva forma de *fake news*, han llegado con fuerza y atacan en varios frentes. Vistos como una amenaza para las empresas, las organizaciones y las marcas (Westerlund, 2019; Galston, 2020; Gaimari, 2021; Da Cruz, et al., 2021; García-Ull, 2021; De Brito d'Andréa & Henn, 2021), son usados en guerras de desinformación, pareciendo el equivalente propagandístico de la era de las espadas y los escudos (Chesney & Citron, 2019), porque los contenidos pueden ser peligrosos, de propaganda o de conflicto social (Cerdán Martínez y Padilla Castillo, 2019).

Los *deepfakes*, que comenzaron a ser usados de forma eficiente en campañas publicitarias, también pueden representar una amenaza para la política y la seguridad cibernética, aumentando el fraude y el *cyberbulling* (Dasilva, Ayerdi y Galdospin, 2021).

Atentos a los riesgos, en varios países, inmediatamente se comenzaron a levantar problemas legales sobre su utilización. En los Estados Unidos, varios estados ya han aprobado leyes que regulan los *deepfakes* y otros están preparados para hacerlo. En Europa el uso de esta nueva tecnología no está legislada explícitamente. Así que ni en España ni en Portugal hay legislación específica, aunque en este último país la normativa hace referencia a los vídeos manipulados.

2. Hipótesis

El presente estudio se desarrolló con base en una investigación exploratoria, a partir de dos revisiones bibliográficas: una sobre el tema genérico *deepfakes* y otra con foco en la desinformación corporativa con recurso a *deepfakes*.

Partimos de las siguientes hipótesis:

- Los *deepfakes* son una forma de *fake news*;
- Los *cheap fakes* también son *deepfakes*;
- Los deepfakes pueden ser usados para propagar desinformación;
- Los *deepfakes* son una amenaza para las empresas, las organizaciones y las marcas;
- La difusión de *deepfakes* puede aumentar la desconfianza de los públicos, afectando a las empresas, las organizaciones y las marcas;
- Cuando utilizados en el ámbito publicitario, los *deepfakes* pueden (o no) ser benéficos para las empresas, las organizaciones y las marcas;
- Esta nueva tecnología preocupa porque representa riesgos a varios niveles: política, seguridad cibernética, fraude y *cyberbulling*;
- Se levantan problemas legales sobre la utilización de *deepfakes*.

3. Objetivos

Este artículo se centra en la desinformación para estudiar el impacto de los *deepfakes*, una nueva forma de *fake* news. No pretende enumerar los mecanismos de detección de esta nueva tecnología, sino evidenciar que existe conciencia de que los *deepfakes* pueden ser una amenaza para varios sectores, concretamente para las empresas, las organizaciones y las marcas. En este sentido, el objetivo general es: reunir las evidencias científicas y literarias y proponer una definición única del término.

4. Metodología

Este trabajo se desarrolló a través de una investigación exploratoria, partiendo de una breve revisión de la literatura con base en dos revisiones bibliográficas: una sobre el tema genérico *deepfakes* y otra con foco en la desinformación corporativa con recurso a *deepfakes*, partiendo de la base de la responsabilidad social de la información (Sánchez-Gey, Jiménez-Marín, Román-San-Miguel, 2022).

Así, primeramente, sin un intervalo de tiempo definido, se partió de una revisión bibliográfica sobre una temática generalista (los *deepfakes*) con base en literatura nacional e internacional. El criterio de selección de las fuentes y referencias partía del cumplimiento de la pesquisa de ser referencias y autores localizados en revistas, libros o publicaciones encontradas en las bases de datos científicas: Mendeley y Google Scholar, y enunciando claramente el término '*deepfake*'.

Seguidamente, se analizó la literatura académica emergente sobre desinformación corporativa con recurso a los *deepfakes*. La investigación exploratoria ha permitido seleccionar, durante el mes de febrero de 2022, artículos científicos publicados en español y en portugués, en la plataforma Google Scholar, entre enero de 2021 y febrero del 2022. Los artículos fueron extraídos manualmente y la búsqueda fue restringida a las publicaciones en los últimos 14 meses no sólo por una cuestión de actualidad, pero también porque sentimos necesidad de balizar nuestras pesquisas. Se han utilizado las mismas palabras clave para los dos idiomas y los resultados nos devolvieron un total de 366 artículos. Hemos reducido la muestra excluyendo los libros y los artículos repetidos. Todavía, con recurso al análisis de contenido, la restringimos a estudios que abordan la temática de interés, que está aún poco explorada científicamente. El intuito fue constatar si los artículos referían si los *deepfakes* pueden tener impacto en las empresas, las organizaciones y las marcas. Al final, se recompiló un total de 11 artículos, todos publicados en el año de 2021.

Palabras clave	Resultado total	Artículos de interés
"*deepfake* + empresas"	122	0
"*deepfakes* + empresas"	128	2
"*deep fake* + empresas"	60	1
"*deep fakes* + empresas"	56	4
TOTAL	**366**	**11**

Fuente: Elaboración propia

5. Descripción de la muestra

La muestra final usada para el análisis de contenido se constituye por 11 artículos de interés. Siete están escritos en español y cuatro en portugués. Los estudios en español son mayoritariamente de España (tres), siguiéndose Colombia (dos), México (uno) y Argentina (uno). Todas las investigaciones en portugués son de Brasil, con cuatro artículos.

IDIOMA	DATA PUBLICACIÓN	AUTORES	TÍTULO	BASE DE DATOS	PAÍS
ES	Enero 2021	Arencibia, M. G.Cardero, D. M.	*Soluciones educativas frente a los dilemas éticos del uso de la tecnología deep fake*	Editic - Revista Internacional de Filosofía Teórica y Práctica	Colombia
ES	Enero 2021	Fernández, E. G.	*Análisis forense de imágenes y videos*	Repositorio INFOTEC	México
ES	Marzo 2021	Gaimari, G.	*Inteligencia artificial e impacto en el cibercrimen*	Universidad de Belgrano(Tesis - Grado)	Argentina
ES	Junio 2021	García-*Ull*, F. J.	*Deepfakes: el próximo reto en la detección de noticias falsas*	Analisi.cat (Universidad Barcelona)	España
ES	Septiembre 2021	Bartolomé, M. C.	*Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad*	RESI: Revista de estudios en seguridad internacional. Universidad de la Rioja	España
ES	Diciembre 2021	Almanza, A. R.	*El poder del algoritmo y la vida social*	Revista SISTEMAS. Asociación Colombiana de Ingenieros de Sistemas	Colombia
ES	Noviembre 2021	Romero, J. C.	*Ciberseguridad: Evolución y tendencias*	RESI: Revista de estudios en seguridad internacional. Universidad de la Rioja	España

IDIOMA	DATA PUBLICACIÓN	AUTORES	TÍTULO	BASE DE DATOS	PAÍS
PT	Marzo 2021	Malheiros, N. D. T.	*O Futuro Chegou: Regulamentação Do Uso De Veículos Autônomos No Brasil*	UNIALFA - Centro Universitário Alves Faria(Tesis – Maestría)	Brasil
PT	Mayo 2021	De Brito d'Andréa, C. F.Henn, R	*Desinformação, plataformas, pandemia: um panorama e novos desafios de pesquisa*	Revista Fronteiras Unisinos - Universidade do Vale do Rio dos Sinos	Brasil
PT	Noviembre 2021	Cafeo, C. G.	*Tribunal Superior Eleitoral e o enfrentamento à desinformação nas eleições municipais de 2020*	Unesp - Universidade Estadual Paulista(Tesis – Maestría)	Brasil
PT	Octubre 2021	Santaella, L.De Matto Salgado, M.	Deepfake e as consequências sociais da mecanização da desconfiança	TECCOGS. PUC-SP - Pontifícia Universidade Católica de São Paulo	Brasil

Fuente: Elaboración propia

5. Resultados

Las *fake news* son informaciones con contenido intencionalmente falso (Tandoc, Lim y Ling, 2017) que se parecen verdaderas. Son producidas con una clara intención de influenciar a las personas con intereses específicos, que pueden ser políticos, sociales o económicos (Bakir & McStay, 2017).

El término "*fake news"* se ha banalizado, se utiliza de forma abusiva y puede ser malinterpretado (Esteves & Sampaio, 2019). Tal vez por eso mismo, sobre todo en el medio académico, se verifica alguna renuencia a usar el término. Existe incluso una corriente que defiende la supresión o la limitación del uso de la palabra, por ser insuficiente e inadecuada para describir el complejo fenómeno de la desinformación (Zazpe, 2019). La propia Comisión Europea, cuando divulgó el Código de Buenas Prácticas para Combatir la Desinformación en línea, suprimió el concepto de *fake news* de su vocabulario pasando a usar apenas el término desinformación (Magallón-Rosa, 2019).

No obstante, cuando hablamos de desinformación, la palabra *fake news* surge de inmediato, como si no fuéramos capaces de disociar los dos vocablos. La verdad es que si es *fake news* estamos ante el fenómeno de la desinformación. Puede ser información manipulada, noticias falsas, bulos, rumores, propaganda o anuncios publicitarios con contenidos falsos. Y es en este contexto que surgen los *deepfakes*.

Los estudiosos de la desinformación han demostrado interés en esta temática. Por eso mismo, en los últimos años, en las áreas de las ciencias sociales y hasta en los sistemas informáticos, se ha producido investigación interesante sobre los *deepfakes* (Gamir-Ríos y Tarullo, 2022).

5.1. Deepfakes: cuestiones conceptuales

El término "*deepfake*" resulta de una combinación de dos palabras "deep" ("profundo", pero con origen en *deep learning*) y "*fake*" (falso). Los *deepfakes* son medios visuales o de audio manipulados o sintéticos que parecen auténticos, y que presentan a personas que parecen decir o hacer algo que nunca han dicho o hecho, producidos mediante técnicas de inteligencia artificial, como el aprendizaje automático (*machine learning*) y el aprendizaje profundo (*deep learning*) (Djurre et al., 2021).

Un *deepfake* es un vídeo que superpone la cara de una persona en el cuerpo de otra, algo posible gracias a algoritmos gratuitos y fáciles de usar (Cerdán Martínez y Padilla Castillo, 2019).

El primer intento de creación *deepfake* resultó de una aplicación desarrollada en el año 2017 por un usuario de la plataforma Reddit autodenominado "*Deepfakes*" (Cole, 2017) que usó una técnica de *autoencoder*, es decir, codificador automático (Deshmukh & Wankhade, 2021).

El usuario "*Deepfakes*" publicó vídeos pornográficos usando los rostros de celebridades como Aubrey Plaza, Gal Gadot, Maisie Williams, Taylor Swift y Scarlett Johansson, consiguiendo popularidad mediante votaciones (Cole, 2017). Aunque omitiendo su verdadera identidad, prestó declaraciones al periódico Vice y explicó que el software buscaba imágenes de varios archivos bibliotecarios abiertos y que, para crear las caras de las celebridades, usó la búsqueda de imágenes de Google, fotos de archivo y vídeos de YouTube (Cole, 2017).

El concepto de *deepfake* surge después de la generación de textos automatizados y de la generación de las imágenes falsas. En la primera, con recurso al GPT (transformador generativo pre-entrenado), que es un nuevo modelo de inteligencia artificial, es posible generar textos que pueden ser usados de forma engañosa como siendo escritos por humanos. En la segunda, gracias a las redes generativas antagónicas, se pueden crear rostros de personas que no existen (Giansiracusa, 2021).

La tecnología responsable por los *deepfakes* fue desarrollada con recurso a una otra asociada a la inteligencia artificial, denominada GAN – red generativa antagónica. En el método usado, el codificador automático extrae las características ocultas de las imágenes faciales y el decodificador se utiliza para reconstruir las imágenes faciales. Para intercambiar caras entre imágenes de origen e imágenes de destino, se necesitan dos conjuntos de decodificadores de codificador en los que cada par se utiliza para entrenar en un conjunto de imágenes, y los parámetros del codificador se intercalan entre dos conjuntos de redes (Deshmukh & Wankhade, 2021).

En la actualidad, existe una amplia variedad de procedimientos de edición de video a través de *deep learning*, por lo que el término *deepfakes* ya no se refiere solo al tipo de intercambio de caras utilizado en las publicaciones originales de Reddit, sobre todo porque desde entonces es cada vez más fácil crear vídeos falsos, manipulados a través de técnicas de inteligencia artificial (Dasilva, Ayerdi y Galdospin, 2021).

La verdad es que, gracias a la amplia gama de oferta, la técnica usada ha evolucionado y es hoy accesible a todos, desde expertos a principiantes (Deshmukh & Wankhade, 2021).

Es en este contexto que surge el término *cheap fakes*, que es como suele denominarse a las formas de manipulación audiovisual que se basan en software barato y accesible o en ningún software (Paris, Donovan 2019). Son también *deepfakes*, pero hechos por cualquier persona, con recurso a tecnología ordinaria, o sea, son manipulación audiovisual solo que de forma menos sofisticada (Santaella & de Matto Salgado, 2021), pues no requieren de un alto grado de alfabetización digital para su diseño (Gamir-Ríos y Tarullo, 2022).

IROCAMM
VOL. 5, N. 2 - Year 2022
Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

5.2. Deepfakes y desinformación

Desde el punto de vista de la desinformación, los *deepfakes*, una nueva forma de *fake news*, permiten cumplir algunos objetivos políticos y financieros de los interesados, por lo que se espera que esta nueva tecnología se convierta en el principal proceso de difusión intencional de bulos, sobre todo porque estos son más devastadores que los falsos contenidos de textos, audios o imágenes (Masood et al., 2021).

En los últimos tiempos, la forma de generación de *deepfakes* ha avanzado significativamente (Román-San-Miguel, Sánchez-Gey-Valenzuela; Elías, 2022). Los *deepfakes* con vídeos y audio sintetizados, generados por IA, pueden ser usados para propagar desinformación en todo el mundo, sobre todo a través de las redes sociales, por lo que pueden futuramente representar una grave amenaza, en forma de *fake news* (Masood et al., 2021).

Los *deepfakes* se pueden considerar el auge de la desinformación digital y evidencian cambios en el periodismo, porque son la punta del iceberg y dan forma a los desarrollos actuales en el campo de las noticias y los medios. Comprenden fenómenos y desarrollos que incluyen *fake news*, la manipulación de los canales de las redes sociales por parte de *trolls* o robots sociales, o incluso la desconfianza del público en la evidencia científica (Djurre et al. 2021).

Por su gran capacidad de desestabilización, se espera un incremento de *deepfakes* en las campañas de desinformación, pues el uso masivo de redes sociales o la enorme cantidad de información disponible acaba creando un efecto denominado de infoxicación, que permite multiplicar la efectividad de lo pretendido (Romero, 2021).

En cuanto se escribía este artículo, en plena guerra entre Ucrania y Rusia, se subió a un sitio web de noticias ucraniano pirateado un video manipulado del presidente ucraniano Volodymyr Zelensky llamando a sus soldados a deponer las armas. Este es un ejemplo de cómo los *deepfakes* pueden tener gran impacto: es que el video rápidamente se volvió viral a escala mundial y incluso fue transmitido en vivo por "Ukraine-24", una estación de televisión ucraniana (Polígrafo, 2022).

Sobre los *deepfakes,* Maldita.es, un medio de comunicación español dedicado al *fact checking*, que difiere los *deepfakes* de los *cheap fakes* publicó:

> "Aunque en un futuro podrían convertirse en una amenaza real, en la actualidad hay otras técnicas de desinformación mucho menos complejas, pero igual de efectivas que suponen un peligro mayor. (…) los *deepfakes* podrían convertirse en un problema en el futuro cuando se simplifique y abarate su producción, y cuando se creen herramientas que permitan a cualquier persona hacer uno, pero antes hay que combatir otros tipos de desinformación mucho menos complejas que ya están causando serios problemas en la actualidad. Mientras nos preocupamos con los *deepfakes*, los *cheapfakes* hacen estragos" (Maldita.es, 2021).

Pero en la comunicación social, los *deepfakes* no solo se usan para fines maliciosos. También se utilizan para el bien. Por ejemplo, la agencia Reuters se ha asociado con la *startup* Synthesia con el objetivo de utilizar esta tecnología para interpretar y transmitir informaciones de un juego de fútbol en tiempo real, a través de algoritmos, en un vídeo con un pivote artificial (Casimiro, 2020).

IROCAMM
VOL. 5, N. 2 - Year 2022
Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

5.3. Impacto de los deepfakes en las empresas, las organizaciones y las marcas

Algunos autores encaran la tecnología *deepfakes* como una amenaza para las empresas, las organizaciones y las marcas (Westerlund, 2019; Galston, 2020; Gaimari, 2021; Da Cruz, et al., 2021; García-Ull, 2021; De Brito d'Andréa & Henn, 2021).

Esta nueva tecnología se ha comenzado también a usar como una forma de dañar la reputación corporativa, con altas patentes de las empresas y las marcas a supuestamente pronunciarse sobre diversos asuntos (Bécares, 2021).

Es que sofisticados sistemas de clonación de voz pueden ser usados en ataques a las empresas o instituciones gubernamentales (Massod, 2021), así como los videos manipulados, que también pueden ser usados para sabotear a los CEO corporativos y sus empresas (De Brito d'Andréa & Henn, 2021).

Por ejemplo, en marzo de 2019, el director gerente de una compañía de energía británica, creyendo que su jefe estaba hablando con él por teléfono, siguió sus órdenes un viernes por la tarde y transfirió más de 240 mil dólares a una cuenta en Hungría, pero todo no pasaba de una burla y los ladrones habían utilizado software que imitaba la voz y el discurso del ejecutivo máximo de la empresa (Harwell, 2019).

Sobre el risco que corren las empresas, ya en el año 2019, noticias financieras y artículos científicos daban cuenta de que estas prácticas podrían aumentar significativamente y de que podrían poner su foco en las empresas, tratando de manipularlas en sus transacciones financieras y decisiones críticas (La Voz del Interior, 2019; Massod, 2021).

En su tercera edición de la revista PTSOC News, dedicada a la seguridad cibernética, la Asociación DNS.PT alerta que las organizaciones están en peligro porque los *deepfakes* pueden ser usadas por criminosos para atacarlas, lo que se podrá traducir en pérdidas financieras (PTSOC News, 2021).

Por otro lado, importa evidenciar que los medios de comunicación, sobre todo los americanos, así como las empresas de redes sociales y de Internet, como Google, Facebook y Twitter, ya están a tomar medidas necesarias para lidiar con la propagación de esta nueva forma de *fake news*: los medios se enfocan en capacitar a los periodistas para su detección y las plataformas en línea tienden a financiar proyectos de investigación cuyo objetivo es desarrollar o mejorar herramientas de análisis forense de medios (Vizoso, Vaz-Álvarez & López-García, 2021).

Los *deepfakes* son una grande amenaza para la sociedad, para los sistemas políticos y para las empresas porque ejercen presión sobre los periodistas que luchan por filtrar las noticias reales de las falsas, amenazan la seguridad nacional al difundir propaganda que interfiere en las elecciones y dificultan la confianza de los ciudadanos hacia la información de las autoridades, planteando, todavía, problemas de ciberseguridad para las personas y las organizaciones (Westerlund, 2019).

Importa referir que tanto los académicos como la comunidad de inteligencia artificial y el mundo empresarial validan esfuerzos para crear herramientas de detección de *deepfakes* (Wodajo & Atnafu, 2021; Yang, J. et al., 2020; Giansiracusa, 2021; Feng et al., 2021).

IROCAMM
VOL. 5, N. 2 - Year 2022
Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

No obstante, a medida que la tecnología *deepfake* se desarrolla y se difunde, hay cada vez más técnicas para detectar *deepfakes*. Y en simultaneo esas mismas técnicas son un incentivo para crear *deepfakes* que no sean detectables por estas técnicas (Fallis, 2020).

5.3.1. Análisis a artículos científicos en español y en portugués

Un análisis a la muestra seleccionada, que consistió en una selección bibliográfica de artículos científicos en español y portugués que evidencian el impacto de los *deepfakes* en las empresas, las organizaciones y las marcas, permite concluir que la literatura emergente sobre la temática en estudio es bastante escasa cuando comparada con la publicada a nivel internacional. Todavía, hay consciencia sobre los riesgos que el uso de esta nueva tecnología puede causar a nivel corporativo, así como sobre las amenazas que representa a varios niveles. Hay también noción de la importancia de estar en alerta constante, para poder acompañar los avances tecnológicos en esta materia.

También podemos verificar que:

- Durante todo el año de 2021, se publicó en la plataforma Google Scholar más literatura científica sobre la temática en estudio en español que en portugués;
- Los estudios publicados en español son mayoritariamente de España (tres), siguiéndose publicaciones aisladas de otros países de América Latina;
- Todas las publicaciones en portugués son de Brasil.

5.3.1.1. Perspectivas futuras

Es urgente combatir los *deepfakes*, videos manipulados difundidos a través de las redes sociales, que se usan de forma masiva, creándose un efecto denominado de infoxicación (Romero, 2021).

Por su nivel de peligrosidad para falsear la realidad, los *deepfakes* son vistos como una preocupación por el daño que provocan (Arencibia y Cardero, 2021), pues pueden ser usados como una poderosa forma de ataque (Gaimari, 2021).

Como las *fakenews* son actualmente el uso más conocido de la IA como vector de ataque en el cibercrimen, en el futuro, se van a necesitar nuevas tecnologías de detección para mitigar el riesgo de campañas de desinformación y extorsión (Gaimari, 2021).

Sólo de esta forma y con un esfuerzo conjunto los ciudadanos podrán mantener la confianza en las organizaciones, empresas y marcas (Bartolomé, 2021; Cafeo, 2021).

5.4. Deepfakes y publicidad. Pros y contras.

La publicidad vio rápidamente en los *deepfakes* una oportunidad (Kietzmann, Adam & Plangger, 2021). Acciones de cariz promocional o publicitario con figuras emblemáticas del pasado comenzaron a ser usadas para promover marcas o productos (Bécares, 2021).

Uno de los ejemplos más emblemáticos es el de una campaña publicitaria lanzada, en enero de 2021, por la marca cervecera Cruzcampo. Esta fue protagonizada, a través de un *deepfakes*, por Lola Flores, famosa artista española fallecida en 1995, y en cuestión de horas batió *récords* de difusión en los medios digitales, tornándose viral (Palomo-Domínguez, 2021).

Otro ejemplo es el del comercial de la cadena de supermercados Soriana, que, en mayo del 2021, también con recurso a la tecnología *deepfakes,* resucitó a Cantinflas, en un vídeo en el que se ve y oye al artista que falleció el 20 de abril de 1993 (Chesney & Citron, 2019; Soriana, 2021).

Es posible que esta nueva tecnología cambie la publicidad (Kietzmann, Mills & Plangger, 2020) tal como la conocemos porque los *deepfakes* son más creíbles, accesibles y novedosos que las *fakes news* (Vosoughi, Roy & Aral, 2018).

De verdad, la imaginación es fértil en esta área. En enero de 2020, la empresa internacional Doritos se asoció a Sway para lanzar una aplicación de *deepfakes* que permitía a los usuarios, gracias a un sistema de IA, visualizarse a si mismos como celebridades bailando en un anuncio con el rapero Lil Nas X y todavía posibilitaba que compartiesen directamente en Instagram, Snapchat, Twitter y TikTok sus movimientos (Kietzmann, Mills & Plangger, 2020).

Pero no todo es color de rosa. Es que los *deepfakes* permiten diferentes formas de desinformación. Primero, pueden tomar la forma de información errónea (*misinformation*) convincente y la ficción puede volverse indistinguible de los hechos para un ciudadano común. En segundo lugar, la desinformación (información engañosa creada o distribuida con la intención de causar daño) puede complementarse con materiales falsos para aumentar su potencial engañoso. En tercer lugar, los deepfakes se pueden usar en combinación con técnicas políticas de micro-focalización, un método publicitario que puede ser muy eficiente porque los productores pueden enviar *deepfakes* personalizados que resuenan fuertemente junto de una audiencia específica (Djurre et al. 2021).

Los *deepfakes* se difunden fácilmente a través de las redes sociales y de masas, y estos medios están tratando febrilmente de gestionar la proliferación de contenido con autenticidad potencialmente engañosa en sus plataformas. Es que los *deepfakes* presentan tanto amenazas como oportunidades para los anunciantes (Kietzmann, Mills & Plangger, 2020).

Desarrollos tecnológicos recientes, particularmente aquellos que usan la inteligencia artificial y el aprendizaje automático, desafían la noción contemporánea de publicidad y de contenido publicitario (Campbell et al., 2021; Li, 2019), por lo que es importante pensar en posibles implicaciones más amplias del uso de *deepfakes* antes de apresurarse a integrar la nueva y atractiva tecnología (Kietzmann, Mills & Plangger, 2020).

Y la producción y distribución de material publicitario dejó de depender apenas del esfuerzo humano y de herramientas analógicas. Pasó a poder servirse de las innovaciones tecnológicas, que ofrecen una industria publicitaria digital y herramientas automáticas que permiten a los anunciantes automatizar muchos procesos publicitarios y producir "anuncios sintéticos" o anuncios que comprenden contenido basado en la producción artificial y automática, así como en la modificación de datos (Campbell et al., 2021).

Es que la publicidad sintética se refiere a anuncios que se generan o editan mediante la producción y modificación artificial y automática de datos. Por lo general, a través de algoritmos de inteligencia artificial, que permiten falsificaciones profundas mediante las GAN, creándose automáticamente contenidos que representan una versión artificial y falsa de una realidad muy convincente (Campbell et al., 2021).

IROCAMM
VOL. 5, N. 2 - Year 2022
Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

5.5. Otros riesgos: política, seguridad cibernética, fraude y cyberbulling

El fenómeno de los *deepfakes* se ha convertido en una preocupación para algunos gobiernos porque representa una amenaza no solo para la política, pero también por la seguridad cibernética, aumentando el fraude y el *cyberbulling* (Dasilva, Ayerdi y Galdospin, 2021).

Un estudio reciente de la internacional Sensity evidencia que los *deepfakes* de vídeo no consensuados y dañinos creados por expertos se duplican aproximadamente cada seis meses. Y hasta diciembre de 2020 fueron detectados más de 85 mil (Sensity, 2021).

Los delitos cibernéticos con recurso a *deepfakes* preocupan bastante:

> "Las redes generativas antagónicas extendidas al *deep learning* han demostrado su extraordinaria capacidad en los campos de la imagen, el audio y el habla. Pero si la tecnología avanzada nos beneficia, también representa una amenaza para nosotros cuando se usa en delitos cibernéticos" (Yang, J. et al., 2020: 1).

Los *deepfakes*, además de haber despertado la preocupación de todos los organismos involucrados por su posible uso intencional, también representan una amenaza inminente porque pueden ser utilizadas con fines dañinos como el robo de identidad, el *phishing* y la estafa (Wodajo & Atnafu, 2021).

Esto ocurre porque las redes generativas antagónicas y las tecnologías de aprendizaje profundo representan una gran amenaza para la seguridad pública y, infelizmente, los métodos tradicionales de detección de falsificación y manipulación no son suficientes para detectar imágenes o vídeos trabajados a través de esta tecnología (Sun et al., 2021). Y está comprobado que los avances en esta área se han empleado para crear software que puede causar amenazas a la privacidad, la democracia y la seguridad nacional (Nguyen et al., 2021).

Altas autoridades policiales también se muestran preocupadas y como tal atentas a los peligros que los *deepfakes* representan. Una información del FBI, publicada en marzo de 2021, deja alertas sobre la posibilidad de actores maliciosos utilizar contenido sintético para operaciones cibernéticas e influencia extranjera en los próximos doce a dieciocho meses:

> "Los actores extranjeros están utilizando actualmente contenido sintético en sus campañas para influir, y el FBI predice que será cada vez más utilizado por actores cibernéticos y delincuentes extranjeros para el *spearphishing* y la ingeniería social en una evolución del comercio cibernético operativo" (FBI, 2021).

También un informe de la Europol sobre la "Evaluación de amenazas de delitos graves y organizados", publicado en abril del mismo año, espera un aumento del uso de *deepfakes* en el crimen cibernético:

> "Las autoridades policiales tienen poderes limitados para contener la manipulación de información, que puede tomar la forma de intentos de distorsionar el discurso político, manipular las elecciones, erosionar los principios democráticos, sembrar desconfianza en las instituciones, intensificar las divisiones sociales, fomentar la inseguridad y difundir la discriminación y la xenofobia (…). El uso delictivo de la IA, incluida la explotación de *deepfakes*, se espera que aumente en el futuro. La incorporación de la IA a las técnicas existentes puede ampliar el alcance y escalar los ciberataques" (Europol, 2021).

IROCAMM
VOL. 5, N. 2 - Year 2022
Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

5.6. Problemas legales sobre la utilización de deepfakes

Como los *deepfakes* fueron usados inicialmente para vídeos falsos de cariz pornográfico, y luego para campañas políticas esencialmente difamatorias, inmediatamente se levantaron varios problemas legales sobre su utilización (Kugler & Pace, 2021).

En los Estados Unidos, varios estados ya han aprobado leyes que regulan los *deepfakes* y otros están preparados para hacerlo, por lo que hay una corriente que defiende que las prohibiciones sobre vídeos pornográficos que resulten de *deepfakes* deben recibir el mismo tratamiento bajo la Primera Enmienda que las prohibiciones de la pornografía no consensual, en lugar de ser tratados bajo la menos protectora ley de la difamación (Kugler y Pace, 2021).

> "Los mecanismos legales existentes son insuficientes para abordar la amenaza porque la Sección 230 de la Ley de Decencia en la Comunicación protege a las empresas de redes sociales de la responsabilidad por los *deepfakes* difundidos en sus plataformas. Incluso las enmiendas propuestas a la Sección 230 no abordan adecuadamente la amenaza de los *deepfakes* (…). Las agencias reguladoras deberían promulgar nuevas reglas y enmendar las existentes para responsabilizar a las empresas de redes sociales por la circulación de deepfakes. La amenaza de responsabilidad disuadirá a las empresas de redes sociales de permitir que los videos se propaguen sin control en sus plataformas y las incentivará a desarrollar nueva tecnología para su pronta detección y eliminación" (O'Donnell, 2021).

Por su parte, la Unión Europea aprobó, en abril de 2021, la propuesta de Ley de Inteligencia Artificial que establece en sus disposiciones generales:

> "Normas armonizadas de transparencia aplicables a los sistemas de IA destinados a interactuar con personas físicas, los sistemas de reconocimiento de emociones y los sistemas de categorización biométrica, así como a los sistemas de IA usados para generar o manipular imágenes, archivos de audio o vídeos" (European Comission, 2020).

En las obligaciones de transparencia para determinados sistemas de IA, el reglamento determina que:

> "Los usuarios de un sistema de IA que genere o manipule contenido de imagen, sonido o vídeo que se asemeje notablemente a personas, objetos, lugares u otras entidades o sucesos existentes, y que pueda inducir erróneamente a una persona a pensar que son auténticos o verídicos (ultra falsificación), harán público que el contenido ha sido generado de forma artificial o manipulado" (European Comission, 2020).

Los *deepfakes* no están legislados explícitamente en Europa, ni en España ni en Portugal. Sin embargo, en España, por sus fines, la penalización podría ser por delito contra el derecho a la propia imagen, una injuria o un delito de odio (Cerdán Martínez y Padilla Castillo, 2019).

De esta forma, según en el artículo 18 de la Constitución Española y tipificado en la Ley Orgánica 1/1982, de 5 de mayo, en lo que se refiere a la protección civil del honor, de la intimidad y de la propia imagen, el artículo séptimo establece en sus números 3, 5, 6 y 7 las siguientes intromisiones ilegítimas:

3. "La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo". (…)

IROCAMM
VOL. 5, N. 2 - Year 2022
Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

5. "La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos.
6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.
7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación" (BOE, 14 de mayo de 1982).

En Portugal, en mayo de 2021, se aprobó la Ley n.º 27/2021, con la Carta Portuguesa de Derechos Humanos en la Era Digital. El artículo sexto estabelece, en seis números, el derecho a la protección contra la desinformación:

1. "El Estado vela por el cumplimiento en Portugal del Plan Europeo de Acción contra la Desinformación, con el fin de proteger a la sociedad frente a las personas singulares o colectivas, de jure o de facto, que produzcan, reproduzcan o difundan una narrativa considerada desinformación, de conformidad con el párrafo siguiente.
2. Se considera desinformación cualquier narrativa que se demuestre que es falsa o engañosa, creada, presentada y difundida para obtener una ventaja económica o para engañar deliberadamente al público, y que pueda causar un daño público, es decir, una amenaza a los procesos políticos democráticos, a los procesos de elaboración de políticas públicas y a bienes públicos.
3. A los efectos del párrafo anterior, se considera, entre otras cosas, información demostrablemente falsa o engañosa la utilización de textos o vídeos manipulados o fabricados, así como las prácticas para inundar buzones de correo electrónico y el uso de redes de seguidores ficticios.
4. Los meros errores en la comunicación de información, así como las sátiras o parodias, no están amparados por lo dispuesto en este artículo.
5. Toda persona tiene derecho a presentar y ver evaluadas por la Autoridad Reguladora de los Medios de Comunicación denuncias contra las entidades que realicen los actos previstos en este artículo, aplicándose los medios de acción a que se refiere el artículo 21 y las disposiciones de la Ley n.º 53/2005, de 8 de noviembre, sobre los procedimientos de denuncia y deliberación y el régimen sancionador.
6. El Estado apoya la creación de estructuras para la verificación de hechos por medios debidamente registrados y promueve la atribución de sellos de calidad por parte de entidades confiables y dotadas de la condición de utilidad pública" (Diário da República, 17 de mayo de 2021).

6. Conclusiones

En este trabajo se parte de la asunción de que los *deepfakes*, además de una amenaza social, pueden representar un peligro para las empresas, las organizaciones y las marcas.

Es cierto que tanto los investigadores como el mundo empresarial se comienzan a mostrar atentos a esta realidad, pero la verdad es que esperábamos resultados más animadores, sobre todo porque es una temática bastante tratada en los medios de comunicación social.

Como tal, esperamos que nuestro trabajo sea una contribución o una especie de incentivo para que se produzca más literatura sobre esta temática que aún no ha sido muy explorada.

Todavía, importa subrayar que ni todo es malo cuando se habla de *deepfakes*. Como ha destacado en una entrevista a CNBC, Hao Li, profesor de la Universidad del Sur de California, pionero y experto en la detección de *deepfakes*, esta nueva tecnología también ha sido usada para la creación de aplicaciones positivas (Li, 2019).

IROCAMM
VOL. 5, N. 2 - Year 2022
Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

Efectivamente, para algunas empresas tecnológicas o publicitarias, los *deepfakes* son sinónimo de oportunidad, tanto a nivel de producciones gráficas de audio y de video, como para las interacciones hombre-máquina y la utilización de esta tecnología en videoconferencias (Djurre et al., 2021).

Y hay más perspectivas optimistas: los *deepfakes* pueden ser benéficos si aplicados correctamente en diferentes áreas, como en la educación, el arte y la ciencia (Silbey & Hartzog, 2019), o la propia educomunicación (Elías, Jiménez-Marín, García Medina, 2018).

Esta nueva tecnología puede ser usada para que los jóvenes estudien las culturas del mundo y las humanidades, experimentando el mundo natural. Incluso, si crecen conscientes de la existencia de esta tecnología, que saben que puede ser molesta o divertida, estarán más alertas para su potencial uso prejudicial, convirtiéndose en personas curiosas, colaborativas, escépticas y productivas. La idea es tener la ventaja narrativa para producir pensadores críticos y ganar la batalla por la verdad (Silbey & Hartzog, 2019).

Como vivimos en una era propicia para la desinformación, la solución pasaría por estimular e invertir colectivamente en medios de comunicación más confiables y menos subsidio-dependientes, así como restablecer normas institucionales de autenticación y verificación (ibidem).

Es esencial ser proactivo y no reactivo. Urge entonces seguir desarrollando formas de combate a varios niveles: detección, regulación, alfabetización mediática y educomunicación, entre otros.

7. Referencias

Almanza, A. R. (2021). El poder del algoritmo y la vida social. *Sistemas*, (161), 24-47. https://sistemas.acis.org.co/index.php/sistemas/article/view/166

Arencibia, M. G., & Cardero, D. M. (2021). Soluciones educativas frente a los dilemas éticos del uso de la tecnología deep fake. *Revista Internacional De Filosofía Teórica Y Práctica*, *1*(1), 99-126. http://riftp.editic.net/index.php/riftp/article/view/22

Bakir, V. & McStay, A. (2017). Fake news and The Economy of Emotions: Problems, causes, solutions. *Digital Journalism, 6*(2), 154-175. https://research.bangor.ac.uk/portal/files/19296816/2017_Fake_news.pdf

Bartolomé, M. C. (2021). Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad. *Revista de Estudios en Seguridad Internacional*, *7*(2), 167-185. https://dialnet.unirioja.es/servlet/articulo?codigo=8306043

Bécares, B. (2021). *La historia de cómo un deepfake consiguió dañar la reputación de una empresa de refrescos en España: así son los nuevos ciberdelitos*. Genbeta. https://www.genbeta.com/actualidad/historia-como-deepfake-consiguio-danar-reputacion-empresa-refrescos-espana-asi-nuevos-ciberdelitos

BOE. 1982. *Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*. 14 de mayo de 1982. https://www.boe.es/buscar/doc.php?id=BOE-A-1982-11196

Cafeo, C. G. (2021). *Tribunal Superior Eleitoral e o enfrentamento à desinformação nas eleições municipais de 2020*. Dissertação de Mestrado. Unesp - Universidade Estadual Paulista. Brasil. https://repositorio.unesp.br/handle/11449/215521

Campbell, C., Plangger, K., Sands, S. & Kietzmann, J. (2021) *Preparing for an Era of Deepfakes and AI-Generated Ads: A Framework for Understanding Responses to Manipulated Advertising*. Journal of Advertising. https://doi.org/10.1080/00913367.2021.1909515

Casimiro, J. T. (2020). *'Deepfakes'. Protótipo recorre à inteligência artificial para marcar nova era da informação digital. O Jornal Económico*. https://jornaleconomico.sapo.pt/noticias/reuters-cria-prototipo-de-inteligencia-artificial-que-utiliza-um-clone-digital-para-relatar-jogos-minuto-a-minuto-547042

Cerdán Martínez, V. y Padilla Castillo, G. (2019). Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso, *Historia y comunicación social*, *24* (2), 505-520. https://doi.org/10.5209/hics.66293

Chesney, R., & Citron, D. (2019). *Deepfakes and the new disinformation war: The coming age of post-truth geopolitics*. Foreign Affairs. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war

Cole, S. (2017, 11 de diciembre). AI-Assisted Fake Porn Is Here and We're All Fucked. Vice. https://motherboard.vice.com/en_us/article/gydydm/gal-gadot-fake-ai-porn

Da Cruz, E. P. F., Pereira, R. M., Jubini, G. M., Quarto, L. C., & de Souza, C. H. M. (2021). Fake news: uma revisão compreensiva e interdisciplinar. *Cadernos de Educação Tecnologia e Sociedade*, *14*(3), 502-520. https://brajets.com/v3/index.php/brajets/index

Dasilva, J. P; Ayerdi, K. M. & Galdospin T. M. (2021). *Deepfakes on Twitter: Which Actors Control Their Spread?* Media and Communication, Vol. 9, Issue 1, ISSN: 2183–2439, 301–312. https://doi.org/10.17645/mac.v9i1.3433

De Brito d'Andréa, C. F., & Henn, R. (2021). Desinformação, plataformas, pandemia: um panorama e novos desafios de pesquisa. *Fronteiras-estudos midiáticos*, *23*(2). http://www.revistas.unisinos.br/index.php/fronteiras/article/view/23786

Djurre, D.; Boheemen, P.; Linda, N.; Jahnel, J.; Karaboga, M.; Fatun, M. & Huijstee, M. (2021). *Tackling Deepfakes in European policy*. ISBN: 978-92-846-8400-7. European Parlament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039

Deshmukh A., Wankhade S.B. (2021). *Deepfake Detection Approaches Using Deep Learning: A Systematic Review*. In: Balas V.E., Semwal V.B., Khandare A., Patil M. (eds) *Intelligent Computing and Networking. Lecture Notes in Networks and Systems*, Vol. 146. Springer, Singapore. https://www.springer.com/series/15179

Diário da República. *Lei n.º 27/2021, de 17 de maio. Carta Portuguesa de Direitos* Humanos *na Era Digital.* 17 de maio de 2021. https://dre.pt/dre/detalhe/lei/27-2021-163442504

Elías Zambrano, R.; Jiménez-Marín, G.; García Medina, I. (2018). Educomunicación, televisión y valores. Análisis de la programación desde una óptica publicitaria. *Educação & Linguagem*, *21*(1), 95-107.

Esteves, F. & Sampaio, G. (2019). Viral: a epidemia de fake news e a guerra da desinformação. Porto Salvo, Portugal. Desassossego.

Europol. (2021). *EU Serious and Organised Crime Threat Assessment (SOCTA).* https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021

European Comission. (2020). Proposal for an AI Regulation laying down harmonised rules on artificial intelligence. COM/2021/206 final. https://digital-strategy.ec.europa.eu/news-redirect/709090

Fallis, D. (2020). The Epistemic Threat of Deepfakes. Philosophy & Technology 34:623–643. https://doi.org/10.1007/s13347-020-00419-2

FBI. (2021). *Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations*. https://www.ic3.gov/Media/News/2021/210310-2.pdf

Feng J., Zhang J., Liu M. y Fang Y. (eds). (2021) *Biometric Recognition. CCBR 2021. Lecture Notes*. Computer Science, vol 12878. Springer, Cham. https://doi.org/10.1007/978-3-030-86608-2_38

Fernández, E. G. (2021). *Análisis forense de imágenes y videos*. INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. Mexico. https://infotec.repositorioinstitucional.mx/jspui/handle/1027/475

Gaimari, G. (2021). Inteligencia artificial e impacto en el cibercrimen (Doctoral dissertation, Universidad de Belgrano-Facultad de Derecho y Ciencias Sociales-Abogacía). http://repositorio.ub.edu.ar/handle/123456789/9333

Galston, William (2020), "Is seeing still believing? The Deepfake Challenge to Truth in Politics", *Brookings Institution*, 8/01/2020. https://www.brookings.edu/research/is-seeing-still-believing-the-deepfake-challenge-to-truth-in-politics/

Gamir-Ríos, J., y Tarullo, R. (2022). *Predominio de las cheapfakes en redes sociales. Complejidad técnica y funciones textuales de la desinformación desmentida en Argentina durante 2020*. adComunica, 97-118. https://doi.org/10.6035/adcomunica.6299

García-Ull, F. J. (2021*).* Deepfakes: el próximo reto en la detección de noticias falsas. *Anàlisi: Quaderns de comunicació i cultura*, 64, 103-120. https://dialnet.unirioja.es/servlet/articulo?codigo=7987666

Giansiracusa, N. (2021). *How Algorithms Create and Prevent Fake News: Exploring the Impacts of Social Media, Deepfakes, GPT-3, and More*. Apress. USA. https://link--springer--com.us.debiblio.com/book/10.1007%2F978-1-4842-7155-1

Harwell, D. (2019). *An artificial-intelligence first: Voice-mimicking software reportedly used in a major theft*. https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/

Kietzmann, J., Mills, J. A. & Plangger, K. (2021) *Deepfakes: perspectives on the future "reality" of advertising and branding,* International Journal of Advertising, 40:3, 473-485, https://doi.org/10.1080/02650487.2020.1834211

Kugler, M. B. & Pace, C., (2021). *Deepfake Privacy: Attitudes and Regulation*. Northwestern Public Law Research Paper, Rev. 611 (3), 611-680. http://dx.doi.org/10.2139/ssrn.3781968

La Voz del Interior. (2019). Agencia DPA. 28/11/2019. https://www.lavoz.com.ar/tecnologia/deepfakes-seran-proxima-frontera-del-fraude-empresarial-desde-2020-segun-especialistas/

Li, H. (2019). CNBC Interview. In Stankiewicz, K. *'Perfectly real' deepfakes will arrive in 6 months to a year, technology pioneer Hao Li says*. 29/09/2019. CNBC. https://www.cnbc.com/2019/09/20/hao-li-perfectly-real-deepfakes-will-arrive-in-6-months-to-a-year.html

Magallón-Rosa, R. (2019). *'Unfaking News'. Cómo combatir la desinformación*. Madrid. Pirámide.

Malheiros, N. D. T. (2021). *O Futuro Chegou: Regulamentação Do Uso De Veículos Autônomos* No Brasil. Dissertação de Mestrado. UNIALFA - Centro Universitário Alves Faria. http://tede.unialfa.com.br/jspui/handle/tede/377

Maldita.es. (2021). Por qué los 'deepfakes' no son el problema (aún) y sí los 'cheapfakes'. 21/01/2021. https://maldita.es/malditobulo/20210121/por-que-los-deepfakes-no-son-el-problema-aun/

Masood, M.; Nawaz, M.; Malik, k.; Javed A. & Irtaza, A. (2021). *Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward*. ArXiv [cs.CR] abs/2103.00484. https://arxiv.org/abs/2103.00484

Nguyen, T. T.; Nguyen, Q. V. H.; Nguyen, C. M.; Nguyen D.; Nguyen D. T. & Nahavandi, S. (2021). *Deep Learning for Deepfakes Creation and Detection: A Survey*. ArXiv:1909.11573v3 [cs.CV] 26 apr 2021. https://arxiv.org/pdf/1909.11573.pdf

O'Donnell, N. (2021). *Have we no decency? section 230 and the liability of social media companies for deepfake videos*. University of Illinois Law Review. University of Illinois College of Law. https://www.mendeley.com/catalogue/884efc71-2a10-367c-b15f-2a335b78a3a9/

Palomo-Domínguez, I. (2021). *Del mito a la viralidad. El caso de la campaña de Cruzcampo que resucitó a Lola Flores*. aDResearch: Revista Internacional de Investigación en Comunicación, 2021, no 26, p. 38-58. https://dialnet.unirioja.es/servlet/articulo?codigo=8111888

Paris, B.; Donovan, J. (2021). *Deepfakes and cheap fakes*. Thousand Oaks: Sage (=Data & Society's Media Manipulation research initiative). https://datasociety.net/library/deepfakes-and-cheap-fakes/

Polígrafo. (2022). *Este vídeo em que Zelensky pede aos ucranianos que se rendam é autêntico?* https://poligrafo.sapo.pt/fact-check/este-video-em-que-zelensky-pede-aos-ucranianos-que-se-rendam-e-autentico

PTSOC News. (2021). *Deepfakes: uma nova ciberameaça às organizações*. Associação DNS.PT. 3ª edição. Dezembro 2021.

Román-San-Miguel, A.; Sánchez-Gey-Valenzuela, N.; Elías-Zambrano, R. (2022). Los profesionales de la información y las fake news durante la pandemia del covid-19. *Vivat Academia. Revista de Comunicación*, 155, 131-149.

Romero, J. C. (2021). *Ciberseguridad: Evolución y tendencias*. bie3: Boletín IEEE, (23), 460-494. https://dialnet.unirioja.es/servlet/articulo?codigo=8175398

Sánchez-Gey Valenzuela, N.; Jiménez-Marín, G.; Román-San-Miguel, A. (2022). La responsabilidad social de las empresas audiovisuales. *Prisma Social*, 37, 238-264. https://revistaprismasocial.es/article/view/4549/5316.

Santaella, L. & de Matto Salgado, M. (2021). *Deepfake e as consequências sociais da mecanização da desconfiança*. TECCOGS: Revista Digital de Tecnologias Cognitivas, (23). https://revistas.pucsp.br/index.php/teccogs/article/view/55981/37929

Sensity. 2021. The State of Deepfakes 2020: Updates on Statistics and Trends. https://sensity.ai/reports/

Silbey, J. & Hartzog, W. (2020). *The Upside of Deep Fakes.* Maryland Law Review, [s. l.], v. 78, n. 4, p. 960–966, 2019. https://digitalcommons.law.umaryland.edu/mlr/vol78/iss4/8/

Soriana. (2021). *Soriana La de Todos Los Mexicanos. #LaDeTodosLosMexicanos*. Recuperado de https://www.youtube.com/watch?v=EpzUryzTZGc

Tandoc Jr., E., Lim, Z. & Ling, R. (2017). Defining 'Fake news': A Typology of Scholarly Definitions, *Digital Journalism*, *6*(3): 1-17. https://www.researchgate.net/publication/319383049_Defining_Fake_News_A_typology_of_scholarly_definitions

Thalen, M. (2022). Twitter. https://twitter.com/MikaelThalen/status/1504123674516885507?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1504123674516885507%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fobservador.pt%2F2022%2F03%2F17%2Fdeepfake-video-falso-de-zelensky-a-render-se-colocado-por-hackers-em-televisao-ucraniana%2F

Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

Vizoso, Á.; Vaz-álvarez, M. & López-García, X. (2021). Fighting deepfakes: Media and internet giants' converging and diverging strategies against hi-tech misinformation. *Media and Communication*, *9*(1), 291–300. https://doi.org/10.17645/MAC.V9I1.3494

Vosoughi, S.; Roy, D. & Aral, S. (2018). The spread of true and false news online. *Science*, (359), 1146-1151. https://www.science.org/doi/10.1126/science.aap9559

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, *9*(11). https://timreview.ca/article/1282

Wodajo, D. & Atnafu, S. (2021). Deepfake Video Detection Using Convolutional Vision Transformer. ArXiv:2102.11126 [Cs, Cv]. 11 mar 2021. https://arxiv.org/abs/2102.11126

Yang, J., Shuai Xiao, S., Li, A., Lan, G., Wang, H. (2021). *Detecting fake images by identifying potential texture difference*. Future Generation Computer Systems, Vol. 125. 127-135. ISSN 0167-739X. https://doi.org/10.1016/j.future.2021.06.043

Zazpe, P. R. (2019). *El fenómeno de la desinformación. Análisis crítico y propuestas de actuación desde el ámbito académico (actualizado). Verdad y falsedad de la información*. UNAM, Instituto de Investigaciones Bibliotecológicas y de la Información, 125-142. https://eprints.ucm.es/id/eprint/60713/

Citación: Gomes-Gonçalves, Sónia (2022). Deepfakes: a new form of corporate disinformation. *IROCAMM - International Review Of Communication And Marketing Mix*, *5*(2), 22-38. https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02

IROCAMM
VOL. 5, N. 2 - Year 2022
Received: 11/03/2022 | **Reviewed:** 09/04/2022 | **Accepted:** 09/05/2022 | **Published:** 31/07/2022
DOI: https://dx.doi.org/10.12795/IROCAMM.2022.v05.i02.02
Pp.: 22-38
e-ISSN: 2605-0447

EDITORIAL
UNIVERSIDAD DE SEVILLA