Respuesta del Anti-Corruption Helpdesk

Las noticias falsas, la corrupción y el cumplimiento en el sector privado

Autora: María Constanza Castro, tihelpdesk@transparency.org
Revisores: Christoph M. Abels, Universidad de Potsdam y Gabriela Camacho, Transparency International
Fecha: 15 de octubre de 2024

Resumen:
Esta respuesta del Anti-Corruption Helpdesk pone el foco en la intersección de la información errónea y la desinformación con la corrupción y la lucha contra la corrupción en el sector privado. El documento examina tres nexos clave entre las empresas y la información errónea, según sean consumidoras, productoras o afectadas. Cuando consumen información errónea o desinformación, en particular a través de vulneraciones de datos de fuentes abiertas y contenidos ultrafalsos o *deepfakes*, las empresas se enfrentan a riesgos que perjudican su capacidad para cumplir la legislación anticorrupción y otras normas de integridad empresarial. Las empresas también pueden producir información errónea o desinformación para utilizarla en prácticas como el blanqueo ecológico y el blanqueo reputacional, que facilitan el soborno, el fraude, el blanqueo de capitales y otros delitos financieros. Además, las empresas pueden verse afectadas por campañas de información errónea o desinformación que las presenten falsamente como corruptas o infractoras de la reglamentación y las normas de integridad empresarial.

Advertencia:
Este documento pone el foco en los nexos, riesgos y respuestas relacionados con la información errónea, la desinformación, la corrupción y la lucha contra la corrupción en el sector privado. Sin embargo, no tiene en cuenta a las empresas de medios de comunicación que alojan las plataformas

Consulta

¿Cómo afectan los riesgos de la información errónea, la desinformación y las noticias falsas a las empresas, y qué medidas pueden tomar estas para mitigar dichos riesgos, proteger su reputación y garantizar el cumplimiento de la normativa? Además, ¿cómo tratan esta cuestión la UE y sus Estados miembros? ¿Cuál es la relación entre estos riesgos y el cumplimiento de la normativa de gobernanza, transparencia y lucha contra la corrupción, y cómo pueden afectar a la reputación de las empresas que cotizan en bolsa? ¿Qué estrategias o iniciativas pueden adoptar las empresas para combatir estos riesgos?

Puntos principales

- El término **información errónea** alude a información falsa que se comparte sin intención de engañar ni de causar daño, mientras que la **desinformación** se comparte con la intención de engañar. El término «noticias falsas» o *fake news* se utiliza a menudo en referencia a ambas cosas. Hay estudios que demuestran que la información falsa tiene un 70 % más de probabilidades de compartirse que la información veraz, lo que hace que la información errónea y la desinformación sean cada vez más preocupantes tanto en el sector público como en el privado.
- Los **procedimientos de cumplimiento**, esenciales para que las empresas respeten los requisitos reglamentarios y eviten la corrupción, dependen en gran medida de una información precisa y fiable. Cuando una empresa se lleva a engaño a causa de informaciones erróneas o desinformación, puede que no detecte riesgos de corrupción, exponiéndose a sufrir consecuencias legales como multas o reclamaciones de responsabilidad civil corporativa, así como importantes pérdidas empresariales.
- Las empresas también pueden verse tentadas a **producir desinformación** para utilizarla en prácticas como el blanqueo ecológico para mejorar su imagen, o el blanqueo reputacional para mejorar la imagen de un cliente. Este tipo de desinformación corporativa puede favorecer la corrupción, el blanqueo de capitales y otros delitos financieros.
- Mientras la corrupción solo aparece en una pequeña fracción (menos del 1 %) de las **noticias falsas corporativas**, la información errónea o la desinformación sobre actividades de presión poco éticas y el incumplimiento de normas representan casi el 15 % de las noticias falsas dirigidas contra empresas.
- Las empresas pueden mitigar los riesgos de la información errónea o la desinformación mediante la **capacitación** (por ejemplo, mejorar la detección de información falsa), las **asociaciones** (con organizaciones de verificación de información o empresas de relaciones públicas especializadas en responder a informaciones erróneas) y el **refuerzo de los procedimientos internos** (como la mejora de los protocolos de verificación).

- Las **respuestas gubernamentales** a la información errónea o la desinformación, como el **Reglamento de Servicios Digitales** en la UE, pretenden crear un entorno informativo más limpio, reduciendo los riesgos de que las empresas consuman, produzcan o se vean afectadas por noticias falsas corporativas.

Contenido

Las noticias falsas, la corrupción y el cumplimiento en el sector privado 5

Información errónea, desinformación y corrupción 5
Las empresas como consumidoras de información errónea y desinformación 8

Riesgo 11
Respuesta 13

Las empresas como productoras de desinformación 15

Riesgo 17
Respuesta 19

Las empresas como blanco de las noticias falsas corporativas 20

Riesgos 22
Respuestas 24

Las noticias falsas, la corrupción y el cumplimiento en el sector privado

Información errónea, desinformación y corrupción

La manipulación de la información no es algo nuevo: la propaganda, las teorías conspirativas, los rumores infundados, la publicidad falsa y las mentiras descaradas se han utilizado durante mucho tiempo para tergiversar la realidad con fines políticos, en beneficio privado o por intereses geopolíticos. Pero en la última década, se han acuñado con urgencia términos como «noticias falsas» (*fake news*), «información errónea» y «desinformación». El alcance algorítmico de las redes sociales ha potenciado la difusión de estas distorsiones, que ahora pueden viajar más rápido y más lejos que nunca. El rápido desarrollo de herramientas de inteligencia artificial generativa ha agravado aún más el problema, al facilitar la creación y difusión de desinformación con una engañosa apariencia de veracidad.

El término *fake news* (noticias falsas o fabricadas) alude a noticias publicadas en internet que estéticamente se parecen a las noticias legítimas de los medios generalistas, pero que son fabricadas o extremadamente inexactas (Pennycook & Rand 2020: 389). Por «noticias falsas» se entiende normalmente tanto la información errónea como la desinformación (Aïmeur *et al*. 2023: 31). Mientras la información errónea es información falsa que se comparte sin intención de engañar, y la desinformación es contenido deliberadamente engañoso, las noticias falsas a menudo difuminan los límites entre ambas cosas, ya que es un término que se aplica ampliamente a cualquier tipo de información falsa, sea intencionada o no. Los conceptos básicos de información errónea, desinformación e información maliciosa giran en torno a dos características fundamentales, la autenticidad y la intencionalidad, y las noticias falsas suelen cuestionar ambas cosas (Aïmeur *et al*. 2023: 30).

Aunque la formación de creencias infundadas a causa de noticias falsas requiere la exposición a información inexacta, el acceso a información de alta calidad no es necesariamente el factor principal para evitar tales creencias. Las creencias infundadas se generan normalmente a través de los mismos mecanismos psicológicos que las fundadas, lo que hace que el proceso de formación de creencias pueda verse influenciado por sesgos y atajos cognitivos. A la hora de determinar la veracidad de la información, las personas suelen exhibir un sesgo cognitivo que les lleva a aceptar la

validez de lo que encuentran, basándose en juicios intuitivos o «corazonadas», en lugar de entregarse a un pensamiento más profundo y crítico (Ecker *et al*. 2022; Lewandowsky *et al*. 2012; Cook, Lewandowsky & Ecker 2017).

La información errónea es información falsa que se comparte sin intención de engañar o causar daño. Por ejemplo, el atentado terrorista de 2017 en los Campos Elíseos generó una gran cantidad de información errónea en las redes sociales[1], que difundían información sin confirmar; sin embargo, no hay pruebas de que quienes compartieron esta información tuvieran la intención de causar daño (Seelow 2017). La desinformación implica que se crea y se comparte información falsa con la intención de engañar. Un ejemplo es la creación de una versión falsificada del periódico belga *Le Soir* durante las elecciones presidenciales francesas de 2017, en la que se afirmaba falsamente que Emmanuel Macron estaba siendo financiado por Arabia Saudí (EU vs DisInfo 2017). La información maliciosa es información auténtica generada y compartida con la intención de causar daño. En las mismas elecciones, se filtraron de forma selectiva correos electrónicos privados de un candidato para perjudicar su campaña (Mohan 2017).

Aunque internet y las redes sociales han tenido un efecto democratizador en el acceso a la información y en su producción (Wihbey 2014: 27), este entorno digital también ha acelerado la propagación de información errónea y desinformación. Según un estudio del MIT Media Lab, las mentiras se difunden «más lejos y más rápido, más profunda y más ampliamente que la verdad», y las falsedades tienen «un 70 % más de probabilidades de retuitearse que la verdad» (Vosoughi *et al*. 2018: 1). Las características de los usuarios y la estructura de la red no pudieron explicar la diferencia en la forma de difusión de la verdad y la falsedad, lo que llevó a los investigadores a señalar la novedad como el factor clave. Tanto desde el punto de vista informativo como desde el social, la atención humana gravita hacia los contenidos más novedosos. El estudio descubrió que, con respecto a un mismo tema, los tuits que contenían información falsa eran significativamente más novedosos que los veraces en todas las métricas de novedad, mostrando una singularidad informativa notablemente superior (Vosoughi *et al*. 2018: 5). Además de la hipótesis de la novedad, herramientas como la amplificación fabricada, las cuentas *bots*, la suplantación de fuentes reputadas, la microsegmentación y los *deepfakes* han facilitado aún más la propagación de la información errónea y la desinformación (Colomina *et al*. 2021:16).

La difusión generalizada de información falsa tiene consecuencias de gran alcance. Puede socavar los derechos humanos fundamentales, debilitar las instituciones y erosionar los procesos democráticos. La información errónea y la desinformación pueden confundir o manipular a los ciudadanos (Colomina *et al*. 2021:11; Jones 2019; OSCE 2017), generar desconfianza en las normas, instituciones y políticas internacionales (Bitiukova *et al*. 2019; Bontcheva & Posetti 2020: 19; Ognyanova *et al*.

[1] Según la definición de Carr & Hayes (2015): Las redes sociales son canales de internet que permiten a los usuarios interactuar de forma oportunista y autopresentarse de forma selectiva, en tiempo real o no, con audiencias amplias o reducidas que obtienen valor de los contenidos generados por esos usuarios y de la percepción de la interacción con los demás.

2020: 4), perturbar las elecciones (PACE 2020; Bennett & Livingston 2018) o alimentar la incredulidad ante retos críticos como el cambio climático o las emergencias sanitarias (Bontcheva & Posetti 2020: 19; Burki 2020).

En el ámbito de la lucha contra la corrupción, la falsedad que se encuentra en la información errónea y la desinformación también representa una grave amenaza. Uno de sus impactos más perjudiciales es su capacidad para erosionar la confianza del público en una prensa libre e independiente, una institución clave para denunciar la corrupción y exigir responsabilidades a los Gobiernos (Kossow 2018: 8). A medida que la información errónea y la desinformación minan la credibilidad de los medios de comunicación, su función como pilares de la integridad se debilita, comprometiendo su capacidad para descubrir la corrupción e informar sobre ella con eficacia.

La confianza del público en las organizaciones de noticias ha disminuido considerablemente en los últimos años (Toff *et al*. 2020; Newman *et al*. 2020; Fletcher 2020; Jurkowitz *et al*. 2020). Por ejemplo, la encuesta Gallup de 2023 reveló que, solo por segunda vez (la primera fue en 2022), el porcentaje de estadounidenses que no confían en los medios de comunicación superó al de los que confían mucho o bastante (Brenan 2023). Las noticias falsas agravan este declive tanto directamente, al acusar a los periodistas de parcialidad, complicidad o incompetencia, como indirectamente, al difundir falsas narrativas que contradicen los informes de los medios generalistas. Además, la creciente presencia de información errónea en línea que imita al periodismo legítimo complica aún más el panorama de los medios de comunicación, erosionando la confianza en todas las fuentes de noticias. Los datos indican que la exposición a informaciones erróneas[2] en el mes anterior a las elecciones de 2018 predijo una disminución del 5 % en la confianza de los participantes en los medios de comunicación, independientemente de su ideología política (Ognyanova *et al*. 2020: 3).

Al margen de la prensa, la desinformación puede dañar la reputación de los agentes dedicados a combatir la corrupción, como los organismos anticorrupción y las organizaciones de la sociedad civil. Al poner en duda la legitimidad de los funcionarios y activistas de estos grupos, la desinformación fomenta una atmósfera de desconfianza y escepticismo que merma su capacidad para actuar con eficacia (Kossow 2018: 8). Por ejemplo, en Ucrania, la Agencia Nacional de Prevención de la Corrupción (NACP) presentó los resultados de su investigación de 2023 «Detección y análisis de amenazas informativas rusas sobre corrupción en el espacio mediático ucraniano», que detectó una campaña sistemática de desinformación por parte de cuentas rusas en múltiples plataformas de redes sociales. Esta campaña pretendía cultivar una narrativa de corrupción generalizada en el gobierno ucraniano, incluida la NACP, con el fin de minar su credibilidad (NACP 2024).

Además, los funcionarios corruptos que son objeto de investigación o que se enfrentan a acusaciones pueden explotar el término «noticias falsas» para desacreditar las

[2] La exposición a noticias falsas se determinó a partir del historial de navegación de los participantes. Se consideró que las personas estaban expuestas si habían visitado alguna de las fuentes de una lista de dominios categorizados como noticias falsas (Ognyanova *et al*. 2020:18).

denuncias válidas de corrupción. Esta táctica se utiliza a menudo para desviar la atención y socavar la confianza en las fuentes de la información, en lugar de alterar directamente la comprensión general de la verdad por parte del público. Al poner en duda informes creíbles, estos funcionarios buscan erosionar la confianza en los medios de comunicación o en los organismos de investigación, lo que hace más difícil exigirles responsabilidades (Kossow 2018: 9). Por ejemplo, en 2023, Libia sufrió tormentas sin precedentes que, agravadas por la inadecuada renovación de las infraestructuras y el abuso de los permisos de construcción, causaron inundaciones masivas en la ciudad de Derna. Tras la catástrofe, se publicaron informes que ponían de relieve la falta de una gestión eficaz de la crisis, la negligencia gubernamental y la corrupción generalizada (Megerisi 2023). La plataforma no partidista Tahara, dedicada a contrarrestar la desinformación y los discursos de odio, informó de varios intentos de debilitar estas acusaciones de corrupción tachándolas de falsas (Jagemast 2023).

Por último, la información errónea y la desinformación pueden influir en la agenda pública trivializando o ahogando las denuncias creíbles de corrupción. En un panorama informativo en el que las noticias reales compiten con las narrativas falsas, los esfuerzos auténticos para que los Gobiernos rindan cuentas pueden perder impacto o pasar desapercibidos por completo (Kossow 2018: 11).

Hasta ahora, la mayoría de los esfuerzos que relacionan la información errónea y la desinformación con la corrupción se han centrado en el sector público. Esta respuesta del Anti-Corruption Helpdeskse centra en la intersección de la información errónea y la desinformación con los casos de corrupción y otras vulneraciones de la integridad, así como sus repercusiones en la lucha contra la corrupción en el sector privado. Explora tres nexos: las empresas como consumidoras, productoras o afectadas por información errónea y desinformación.

Las empresas como consumidoras de información errónea y desinformación

Los procedimientos de cumplimiento son cruciales para que las empresas cumplan los requisitos reglamentarios y prevengan la corrupción. Estos procedimientos se refieren a los sistemas, procesos o departamentos de las empresas que garantizan que todas las actividades legales, operativas y financieras se ajustan a las leyes, normas y reglamentos vigentes y a las expectativas del público (Transparency International 2015). En el contexto de la corrupción, los mecanismos de cumplimiento se centran en garantizar que los agentes privados cumplan la legislación anticorrupción, las medidas de transparencia y los protocolos de integridad financiera, al tiempo que se alinean con las políticas oficiales para promover una mayor supervisión, transparencia y rendición de cuentas (Albisu 2020: 2).

Estos procedimientos dependen en gran medida de información precisa y fiable para llevar a cabo evaluaciones de riesgos, investigar a terceros y comprender los entornos

normativos. Sin embargo, cuando la información de la que dependen las empresas se ve comprometida por la desinformación o la información errónea, su capacidad para garantizar un cumplimiento adecuado se ve considerablemente mermada. Por ejemplo, las campañas de desinformación pueden difundir deliberadamente falsas narrativas sobre las prácticas empresariales de un competidor, llevando a las empresas a juzgar erróneamente los riesgos relacionados con asociaciones o inversiones. En otros casos, la información engañosa sobre cambios en la normativa puede llevar a las empresas a pasar por alto requisitos de cumplimiento esenciales, exponiéndolas al riesgo de sanciones. Además, la desinformación puede ocultar los riesgos de corrupción al minimizar o exagerar la integridad de los socios potenciales. Por ejemplo, si una campaña de desinformación orquestada lleva a una empresa a creer que un socio tiene una reputación intachable, puede que formalice acuerdos comerciales que la expongan a riesgos éticos y jurídicos. Estos escenarios ilustran que las consecuencias de la desinformación van más allá del fraude e incluyen graves repercusiones en la gobernanza corporativa y en la toma de decisiones (Institute for Financial Integrity 2024; Hanley-Giersch & Brokes 2024; Mason & Oxnevad 2024; Petratos & Faccia 2023).

La base de cualquier programa de cumplimiento bien diseñado reside en la capacidad de una empresa para determinar, evaluar y definir su perfil de riesgo, así como en la medida en que dicho programa asigna sistemas de control y recursos adecuados para todo el abanico de riesgos. En la evaluación de riesgos de una empresa influyen factores como la ubicación de sus operaciones, el sector industrial, la competitividad del mercado, el panorama normativo, los clientes y socios comerciales potenciales, las transacciones con Gobiernos extranjeros, los pagos a funcionarios extranjeros y el uso de terceros, así como regalos, viajes, gastos de representación y donaciones benéficas o políticas (US DOJ 2023: 3). Cuando la información y los datos en los que se basan estas evaluaciones se ven comprometidos por la información errónea o la desinformación, puede que se reste importancia a los riesgos y se cree una falsa sensación de seguridad que lleve a las empresas a aplicar controles de cumplimiento menos estrictos.

La distinción entre desinformación y fraude suele ser tenue. Esta ambigüedad ha llevado a algunos juristas a abogar por la aplicación de marcos jurídicos que traten la desinformación como una forma de fraude contra el público. Estos marcos obligarían a los autores de la desinformación a rendir cuentas del daño causado por su difusión deliberada, haciéndoles responsables ante los perjudicados (Henriksen 2022).

Otro aspecto crítico del cumplimiento que es vulnerable a la información errónea o la desinformación es la diligencia debida con respecto al cliente (DDC) y los procedimientos «conozca a su cliente» (KYC) (US DOJ 2023: 7). Las empresas recurren a estos procesos para efectuar averiguaciones sobre posibles socios, clientes e inversiones, a menudo utilizando fuentes de información externas como artículos de prensa, informes y bases de datos en línea. Cuando estas fuentes contienen información inexacta o engañosa, a menudo difundida deliberadamente por agentes malintencionados o involuntariamente a través de campañas de información errónea,

la integridad de estos procedimientos puede verse comprometida. Por ejemplo, una empresa puede suscribir, sin saberlo, acuerdos con socios que han utilizado la desinformación para ocultar riesgos de corrupción, lo que puede acarrear daños para su reputación y consecuencias legales. Además, la desinformación puede afectar significativamente a la gestión de la cadena de suministro al ocultar las verdaderas prácticas y la integridad de los proveedores o subcontratistas. Puede ocurrir que las empresas confíen en información engañosa que presente a los proveedores como cumplidores y éticos, de modo que se omitan auditorías o se realicen labores de supervisión inadecuadas (Petratos & Faccia 2023).

Por último, la exposición a la desinformación puede distorsionar la capacidad de una empresa para evaluar su cumplimiento de la normativa. Por ejemplo, en 2018, un memorándum falsificado del Departamento de Defensa de EE. UU. afirmaba fraudulentamente que la adquisición de otra empresa tecnológica por parte de un gigante de los semiconductores vulneraba la normativa y planteaba problemas de seguridad nacional. Este memorándum falso no solo provocó la caída de las cotizaciones bursátiles de ambas empresas, sino que también hizo que sus conversaciones sobre una posible fusión quedasen paralizadas (Reuters 2018).

Una parte considerable de los procedimientos de cumplimiento de una empresa depende a menudo de información de dominio público, y la inteligencia de fuentes abiertas (OSINT) se perfila como una herramienta vital en los procesos de cumplimiento modernos. La inteligencia de fuentes abiertas se obtiene mediante la recopilación y el análisis sistemáticos de información de dominio público procedente de diversas fuentes, como plataformas en línea, medios de comunicación, registros gubernamentales y bases de datos reglamentarias. Esta abundancia de datos constituye un valioso recurso para las organizaciones que desean mejorar sus esfuerzos de cumplimiento de la normativa anticorrupción, por ejemplo, mediante el análisis de las estructuras de propiedad y corporativas, la investigación de personas con responsabilidad pública, la vigilancia de anomalías en las transacciones y la detección de indicadores de corrupción en los medios de comunicación (Khavanov 2024). Aunque la inteligencia de fuentes abiertas puede ser una herramienta para hacer frente a la información errónea y la desinformación (Innes y Dawson 2023), su condición de fuente abierta también hace que sea vulnerable a la información errónea o la desinformación (Kemsley, Corbett y Cooke 2024).

El riesgo de que las empresas caigan en la desinformación se ve exacerbado por el auge de los modelos de desinformación como servicio (DaaS), que se utilizan específicamente para crear identidades falsas en las redes sociales (Bank of America 2023a: 2). Estas identidades pueden utilizarse para mejorar una reputación mediante la fabricación de reseñas, testimonios y noticias, o también para dañarla utilizando las mismas tácticas. La DaaS puede afectar tanto a particulares como a organizaciones, a menudo con un coste relativamente bajo: desde menos de 100 hasta unos 100 000 dólares (Bank of America 2023a: 2). La DaaS puede producir y difundir desinformación a través de varios canales, siendo los más frecuentes las redes sociales (mediante mensajes o cuentas falsas), así como a través de sitios web *proxy* o falsos diseñados

para ocultar la fuente del contenido o para atraer visitas a la página. Además, la DaaS puede aprovechar herramientas como las granjas de contenidos y las redes de *bots*. Las granjas de contenidos generan grandes volúmenes de contenidos web de baja calidad con fines de optimización para motores de búsqueda (SEO), es decir, para lograr mejores posiciones en los resultados de búsqueda. Las redes de *bots* consisten en redes de ordenadores infectados con software malicioso o *malware* y controlados por una única entidad, lo que permite realizar acciones coordinadas que amplifican la desinformación a escala masiva (Bank of America 2023a: 2).

Otra preocupación creciente en el ámbito del cumplimiento es el uso de *deepfakes* (contenidos ultrafalsos) para facilitar actividades corruptas o delictivas mediante la falsificación de identidades en línea y la elusión de los mecanismos KYC (Europol 2022: 10). Los *deepfakes* —vídeos, audios, fotos y textos creados mediante inteligencia artificial— son extremadamente difíciles de diferenciar de los contenidos auténticos (Bank of America 2023b: 3). Los métodos actuales de verificación KYC incluyen hacerse un selfi mientras se sostiene un cartel escrito a mano con la fecha actual, sacar una foto del carné de conducir del usuario u otro documento de identidad oficial, y grabar un vídeo en directo en el que los usuarios responden a preguntas de seguridad para confirmar su identidad y presencia física o *liveness*. Sin embargo, ahora todos estos mecanismos pueden sortearse fácilmente mediante la IA generativa. Al parecer, OnlyFake —un servicio de IA que crea carnés de identidad falsos— ha superado estrictos controles KYC en las principales bolsas de criptodivisas, como Binance y Coinbase. Estos carnés falsos, generados mediante redes neuronales, pueden comprarse por tan solo 15 dólares (Ho 2024).

Los *deepfakes* también pueden utilizarse en métodos de compromiso de la identidad empresarial (BIC). Estos métodos utilizan tecnología *deepfake* para crear personajes corporativos sintéticos o imitar a empleados existentes, a menudo haciéndose pasar por un profesional conocido y de alto rango en la organización. En 2020, se utilizó un audio *deepfake* para amenazar al director de un banco de Hong Kong con el fin de que desviara 35 millones de dólares, la mayor pérdida económica causada por contenido no auténtico que se conozca públicamente hasta la fecha (Bank of America 2023b: 3).

Riesgo

El principal riesgo para las empresas que son víctimas de información errónea o desinformación en sus procedimientos de cumplimiento es que no apliquen las salvaguardias contra la corrupción y la normativa contra el blanqueo de capitales. Esta omisiones no sólo perjudican la responsabilidad social corporativa de una empresa —el deber de actuar en el mejor interés no sólo de su negocio, sino también de las personas, del planeta y de la sociedad en general—, sino que también afectan negativamente a sus operaciones. Numerosas pruebas demuestran que la lucha contra la corrupción no solo es un imperativo ético, sino que también tiene mucho sentido desde el punto de vista empresarial (Bbaale & Okumu 2018; DeRosa, Gooroochurn & Holger 2015; Dutta & Sobel 2016; Martins, Cerdeira & Teixeira 2020; Serafeim 2014; Va Vu *et al*. 2018; Wang 2021; Wegner, Schöberlein & Biermann 2013: 64). Por el contrario,

un programa de ética y cumplimiento anticorrupción mal ejecutado puede acarrear importantes pérdidas con el paso del tiempo, dañando en última instancia la reputación de la empresa, erosionando la confianza de las partes interesadas y comprometiendo su eficacia operativa general (UNODC 2013: 10).

Riesgos jurídicos

Ante todo, las empresas que consumen información errónea o desinformación como parte de sus procedimientos de cumplimiento corren el riesgo de infringir la ley al participar en actos de corrupción, blanqueo de capitales u otros delitos financieros. Estas acciones conllevan graves consecuencias jurídicas, que van desde importantes sanciones económicas hasta la responsabilidad penal de las empresas. El marco jurídico que sustenta estas obligaciones varía según las jurisdicciones, pero está establecido por una serie de leyes pertinentes. Por ejemplo, la Ley estadounidense de prácticas corruptas en el extranjero (FCPA), la Ley británica de delincuencia económica y transparencia corporativa (ECCTA) y la sexta Directiva de la UE contra el blanqueo de capitales (6AMLD), junto con la Directiva sobre diligencia debida de las empresas en materia de sostenibilidad (CS3D), imponen estrictos requisitos de cumplimiento que las empresas deben aplicar cuidadosamente.

La solidez de los mecanismos de cumplimiento es especialmente crítica en determinadas legislaciones. Por ejemplo, en virtud de la Ley británica de delincuencia económica y transparencia corporativa de 2023, el modelo de responsabilidad por omisión de prevención —similar a la responsabilidad penal objetiva— no requiere intencionalidad por parte de la empresa para que se la declare culpable. Si los procedimientos se consideran «inadecuados» o «poco razonables», posiblemente por haber confiado en información falsa, la alta dirección puede ser considerada responsable en casos de fraude, soborno u otros delitos económicos (Randhawa *et al.* 2023).

Riesgos empresariales

Una estrategia de cumplimiento mal aconsejada puede llevar a las empresas a contraer costes innecesarios. Existen abundantes datos que demuestran que el cumplimiento de la normativa anticorrupción por parte de las empresas está claramente justificado desde el punto de vista económico (Bbaale & Okumu 2018; DeRosa, Gooroochurn & Holger 2015; Dutta & Sobel 2016; Martins, Cerdeira & Teixeira 2020; Serafeim 2014; Va Vu *et al.* 2018; Wang 2021). Participar en la corrupción es costoso para las empresas. Por ejemplo, a partir de una muestra de 21 250 empresas ubicadas en 117 países emergentes y en desarrollo, y utilizando estimaciones de variables instrumentales, se ha descubierto que, independientemente de la variable sustitutiva que se utilice para la corrupción y el rendimiento de la empresa, la primera perjudica claramente al segundo (Martins, Cerdeira & Teixeira 2020). Un estudio de la OCDE (2014: 8) señala además que el soborno, junto con las prolongadas negociaciones que suele conllevar, eleva los costes empresariales. Por término medio, los sobornos representan el 10,9 % del valor de una transacción y un asombroso 34,5 % de los beneficios.

Cuando se detecta corrupción, las sanciones añaden costes sustanciales al gasto inicial del soborno. En la UE, por ejemplo, el Consejo ha acordado recientemente su posición con respecto a una legislación que podría imponer importantes sanciones a las personas jurídicas —como las empresas— que sean declaradas culpables de delitos de corrupción. Estas sanciones podrían incluir multas del 3 al 5 % del volumen de negocios total de la empresa a escala mundial o multas mínimas de 24 a 40 millones de euros, en función de la gravedad del delito (Consejo de la UE 2024).

Al margen de los costes financieros directos, unos mecanismos de cumplimiento anticorrupción deficientes pueden acarrear importantes costes indirectos. Los costes de «limpieza», como honorarios de abogados, auditorías e investigaciones, así como los gastos de las medidas correctoras, pueden ser millonarios y afectar seriamente a los resultados financieros de una empresa. Los costes indirectos a largo plazo por incumplimiento de las medidas anticorrupción incluyen la pérdida de confianza de accionistas e inversores, un acceso reducido a capital, daños reputacionales y efectos perjudiciales para la moral del personal (Jenkins 2018: 8). Por ejemplo, un estudio reveló que las cotizaciones bursátiles de las empresas procesadas por soborno en el extranjero cayeron una media del 3,11 % el primer día de la actuación policial y un 8,98 % en el transcurso de la misma (Karpoff, Lee & Martin 2013).

Respuesta

Contrarrestar el consumo de información errónea y desinformación depende en gran medida de la capacidad de detectarla con precisión. Sin embargo, datos recientes de la OCDE indican que a menudo no existe correlación entre la capacidad percibida para detectar contenidos falsos o engañosos en internet y la habilidad real para hacerlo. De hecho, las personas encuestadas en un estudio solo distinguieron los contenidos verdaderos de los falsos el 60 % de las veces, siendo las afirmaciones verdaderas más difíciles de detectar que las falsas (OCDE 2024). Para salvar esta brecha, las empresas pueden adoptar diversas estrategias, desde la formación de los empleados hasta la inversión en herramientas tecnológicas que automaticen en cierta medida la detección de la información errónea y la desinformación. Ejemplos de este tipo de herramientas son Fact Check Explorer de Google, que ayuda a los usuarios a cotejar alegaciones con una base de datos de artículos verificados, y ClaimReview, que permite que las organizaciones etiqueten dichas alegaciones como verificadas para facilitar su identificación en línea. Además, plataformas como Media Bias/Fact Check y NewsGuard ofrecen evaluaciones de la credibilidad de las fuentes de noticias, lo que permite a las empresas tomar decisiones fundamentadas sobre la información que consumen y comparten.

Formación para responsables de cumplimiento

Los responsables de cumplimiento y otros empleados encargados de los procedimientos anticorrupción deben estar bien informados sobre los riesgos asociados a la información errónea y la desinformación en relación con su trabajo.

Además de aumentar la sensibilización, las empresas pueden invertir en la creación de capacidades para detectar con precisión las noticias falsas y otros tipos de información errónea y desinformación (Mason & Oxnevad 2024). A medida que se perfeccionen los *deepfakes*, será cada vez más difícil distinguirlos de los contenidos auténticos. Sin embargo, las personas todavía pueden detectar contenidos sintéticos creados con tecnología *deepfake* rudimentaria o por autores de amenazas menos capacitados. La formación en detección de *deepfakes* puede mejorar la probabilidad de que los empleados detecten tentativas antes de que causen daños (Bank of America 2023b: 5).

Respetar las mejores prácticas de ciberseguridad

Reforzar las medidas de ciberseguridad es esencial para combatir la desinformación, que se ha revelado sistemáticamente como una amenaza omnipresente en el espacio digital. La difusión y persistencia de la desinformación, especialmente en las plataformas de redes sociales, representa una de las amenazas más problemáticas tanto para los usuarios como para los administradores de contenidos (Caramancion 2020). Todos los empleados deben comprender bien las políticas de seguridad fundamentales, en particular la importancia de examinar las comunicaciones sospechosas y verificar su autenticidad a través de canales secundarios. Se debe animar a los empleados a tomarse un momento para reflexionar y transmitir sus dudas con respecto a la validación de comunicaciones potencialmente falsas, especialmente las que solicitan información sensible o pagos al margen de los procedimientos habituales. También debe proporcionarse un refuerzo positivo cuando los empleados logren detectar información falsa y evitar pérdidas (Bank of America 2023b: 4).

Las empresas también pueden aprovechar las principales características de la tecnología de cadena de bloques —descentralización, inmutabilidad y consenso basado en reglas— para reforzar los procesos de verificación de identidad y detección del fraude. El carácter descentralizado de la cadena de bloques, por la que se distribuyen los datos a través de una red de nodos, garantiza que sea sumamente difícil realizar cambios no autorizados, ya que cualquier modificación requeriría el consenso de la mayoría de los nodos. Además, como los registros de cadena de bloques son inmutables, una vez que se registra una transacción o un dato, no puede alterarse sin dejar rastro, lo que añade una capa de confianza y transparencia (Dai, Wang y Vasarhelyi 2017).

Esta misma tecnología podría aplicarse a la certificación de la autenticidad de la información. Utilizando la cadena de bloques para registrar y rastrear el origen y la verificación de los datos, las empresas podrían consumir información certificada como auténtica y trazable. La cadena de bloques puede proporcionar una cadena de custodia verificable para la información, que garantice que cualquier contenido compartido o utilizado por una empresa pueda rastrearse hasta su fuente y pueda validarse su exactitud. Algoritmos criptográficos como las funciones *hash* pueden crear firmas digitales únicas para la información, con el fin de detectar cualquier manipulación y garantizar su integridad (Ho 2024; Petratos & Faccia 2023). Este método ayudaría a las

empresas a asegurarse de que los datos en los que se basan son creíbles, reduciendo así el riesgo de ser víctimas de informaciones erróneas o desinformación.

Las empresas como productoras de desinformación

Las empresas pueden favorecer los comportamientos corruptos produciendo desinformación, bien sobre sí mismas o bien sobre terceros, con fines comerciales o financieros. Las empresas pueden tener la tentación de manipular la verdad o de hacer afirmaciones exageradas para alcanzar objetivos y parámetros financieros. Para las empresas, la línea que separa la persuasión del engaño puede ser fina en lo que respecta a sus productos o servicios, pero quizá sea más problemática en lo que se refiere a sus esfuerzos de cumplimiento (Leighton 2023).

Un ejemplo común es el «blanqueo ecológico» o *greenwashing*, por el que las empresas exageran o falsifican las alegaciones sobre sus prácticas ambientales, sociales y de gobernanza (ASG) para parecer más respetuosas con el clima y el medio ambiente. Las empresas que practican el blanqueo ecológico intentan presentarse como sostenibles, a menudo con campañas dirigidas de publicidad y relaciones públicas, en lugar de efectivamente establecer prioridades sostenibles (Lescher 2023). Algunos académicos han considerado este comportamiento como un tipo de desinformación corporativa, ya que existen incentivos reputacionales y financieros para que las empresas se beneficien de la difusión de esta información falsa (Naderer, Martens & Schmuck 2017; Naderer & Opree 2021; Medeiros *et al*. 2024). Al manipular las narrativas acerca de sus esfuerzos de sostenibilidad, las empresas pueden evitar el control y eludir la rendición de cuentas, al tiempo que cosechan los beneficios —como su inclusión en fondos de inversión sostenibles— de lograr una reputación ecológica sin haber realizado un verdadero esfuerzo de responsabilidad medioambiental (de Freitas Netto *et al*. 2020; Laufer 2003; Naderer, Martens & Schmuck 2017). Un fenómeno similar, a menudo descrito como *bluewashing*, consiste en que las empresas producen desinformación estratégicamente para evitar o tergiversar los compromisos de responsabilidad social empresarial (RSE) (Bennet & Uldman 2024, McClimon 2022).

El escándalo de las emisiones de Volkswagen (VW), también conocido como *Dieselgate*, es un buen ejemplo de blanqueo ecológico corporativo como estrategia de desinformación para eludir la regulación. En 2015, se reveló que VW había instalado *software* en millones de vehículos diésel para trucar los ensayos de emisiones, haciendo que los coches parecieran cumplir las normas medioambientales cuando, en realidad, emitían óxidos de nitrógeno hasta 40 veces por encima del límite legal (Hotten 2015). Este engaño deliberado permitió a VW comercializar estos vehículos como «ecológicos» mientras eludía reglamentaciones más estrictas destinadas a reducir la contaminación. La campaña de desinformación de la empresa no solo llevó a engaño a reguladores y consumidores, sino que también distorsionó la competencia en el

mercado, ya que se presentó falsamente como líder en innovación medioambiental (Naderer, Martens & Schmuck 2017).

En un documento de trabajo conjunto de la Universidad de Harvard y el Algorithmic Transparency Institute, los investigadores realizaron un análisis de contenido textual y visual de 2 325 publicaciones orgánicas en redes sociales de 22 grandes productores de combustibles fósiles, fabricantes de automóviles y compañías aéreas con sede en la Unión Europea. Dichas publicaciones, compartidas en Facebook, Instagram, TikTok, Twitter y YouTube durante el verano de 2022, revelaron que dos tercios del contenido de las redes sociales de las empresas de petróleo y gas (72 %), automoción (60 %) y transporte aéreo (60 %) promovían una narrativa de «innovación ecológica», mientras prestaban menos atención a sus operaciones tradicionales. La proporción de comunicaciones que pasan de «verde a sucio» en estas industrias —3 a 1 en el petróleo y el gas, 4 a 1 en la automoción y 1,2 a 1 en el transporte aéreo— no representa sus compromisos actuales con la descarbonización, lo que indica que al menos parte de este contenido constituye blanqueo ecológico (Supran 2022: 3).

Desde finales de la década de 1980, los grupos de interés en los combustibles fósiles —incluidas las empresas de carbón, petróleo, gas, automoción y servicios públicos de suministro—, apoyados por empresas de relaciones públicas, han llevado a cabo una campaña de presión, desinformación y propaganda de varias décadas y miles de millones de dólares con el objetivo de sabotear la ciencia, engañar al público y menoscabar las políticas sobre el clima y las energías limpias (Bonneuil, Choquet y Franta 2021; Cook *et al*. 2019; Dunlop & MccCright 2011; Franta 2021; Supran & Oreskes 2021; Union of Concerned Scientist 2007; Williams *et al*. 2022). Las conclusiones de este estudio se suman a un creciente conjunto de datos que demuestran cómo han evolucionado sus tácticas y su retórica, pasando de una abierta negación climática en prensa y televisión a una desinformación más sutil en las redes sociales y a través de la publicidad nativa en los sitios web de noticias (Cahill 2017; Coan *et al*. 2021; Lamb *et al*. 2020; Nisbet 2009; Schneider *et al*. 2016).

El blanqueo reputacional es una industria creciente de abogados, contables, empresas de relaciones públicas y asesores de imagen que guían y aconsejan a diversos agentes —entre los que se incluyen figuras cleptocráticas y personas con responsabilidad pública corruptas— a través de un proceso de cambio de imagen que a menudo implica hacer grandes donaciones a organizaciones benéficas, universidades y partidos políticos, comprar la ciudadanía mediante «visados de oro», incorporar políticos a consejos de administración, y colocar artículos favorecedores en publicaciones de alto perfil (Wolcott 2022). Aunque hay quien puede argumentar que estas acciones entran dentro de las relaciones públicas legítimas, cabe calificarlas de desinformación cuando se oculta deliberadamente información clave y se promueven narrativas falsas o engañosas. Los profesionales del blanqueo reputacional no se limitan a gestionar la percepción pública, sino que distorsionan activamente la verdad omitiendo o restando importancia a comportamientos corruptos o ilegales, al tiempo que amplifican narrativas artificiosas destinadas a engañar al público sobre la integridad de sus clientes.

Esto es especialmente preocupante cuando las propias empresas participan en el control de medios de comunicación o ejercen presión para suprimir la cobertura negativa, lo que difumina aún más la línea que separa las relaciones públicas de la desinformación. A diferencia de las relaciones públicas tradicionales, que buscan mejorar la reputación basándose en las auténticas fortalezas de una empresa, el blanqueo reputacional fabrica una identidad falsa preparando selectivamente información para engañar al público y a los reguladores. Además, estos esfuerzos crean una ilusión de credibilidad que puede tener consecuencias en el mundo real, por ejemplo menoscabar los procesos de diligencia debida y permitir que los agentes corruptos eludan las sanciones o el control legal. Esta manipulación de los hechos puede limitar gravemente la eficacia de los equipos de cumplimiento, dificultando que las empresas y los Gobiernos detecten los verdaderos riesgos asociados a las personas de alto perfil (Prelec 2022 ; Wolcott 2022).

Las empresas también pueden utilizar la desinformación con fines de sabotaje comercial, difundiendo información falsa sobre sus competidores para menoscabar su reputación o debilitar su posición en el mercado. Por ejemplo, una empresa podría propagar alegaciones engañosas sobre la salud financiera, la seguridad de los productos o las normas éticas de un competidor con el fin de dañar su credibilidad y generar desconfianza. Esta forma de desinformación puede acarrear importantes pérdidas económicas a los competidores, al tiempo que proporciona al productor de la desinformación una ventaja desleal en el mercado. Un estudio de países de Europa del Este halló casos de sobornos a periodistas para que publicasen noticias falsas destinadas a perjudicar a rivales comerciales, unidos a una segunda forma de corrupción: el soborno a funcionarios públicos para fabricar procedimientos judiciales contra competidores comerciales (Teichmann, Ruxandra & Sergei 2022).

Riesgo

Riesgo de ser descubiertas

El riesgo más inmediato para las empresas que producen desinformación es el daño que sufrirá su reputación si sus acciones salen a la luz. Las empresas a las que se descubre desinformando —ya sea a través del blanqueo ecológico, el blanqueo reputacional o los ataques engañosos a la competencia— puede perder la confianza de partes interesadas clave como inversores, clientes y socios comerciales. Esta erosión de la confianza puede acarrear pérdidas financieras, una disminución de la cuota de mercado y un perjuicio a largo plazo para el valor de la marca (Lescher & Kunzmann 2024).

Al margen del daño a su reputación, las empresas que utilizan la desinformación pueden enfrentarse a responsabilidades legales, multas e incluso penas de cárcel. Ejemplos notables son Volkswagen, que fue multada con 34 690 millones de dólares por implementar un *software* que falsificaba los datos de emisiones; Toyota, multada

con 180 millones de dólares por retrasar la presentación de informes relacionados con las emisiones; y DWS, multada con 25 millones de dólares por comercializar fondos ASG como «más verdes» de lo que eran en realidad (Davison 2024). En términos de responsabilidad personal,
el Departamento de Justicia de EE. UU. detuvo y acusó en 2017 a seis ejecutivos de Volkswagen en relación con la conspiración para hacer trampa en los ensayos de emisiones estadounidenses haciendo declaraciones falsas a los reguladores y al público sobre la capacidad de los vehículos de VW que supuestamente funcionaban con «diésel limpio» (US DOJ 2017).

En 2023, la Comisión Federal de Comercio (FTC) de EE. UU. actualizó sus «Guías Verdes» para proporcionar a la agencia argumentos jurídicos más sólidos contra los contaminadores al aclarar cuándo el marketing engañoso de las empresas acerca de la sostenibilidad y la responsabilidad medioambiental infringe la legislación federal. Aunque la FTC presenta contadas demandas, en algunos casos ha impuesto a las empresas multas millonarias. En 2021, por ejemplo, multó a distintas empresas, entre ellas Walmart y Kohl's, con un total de 5,5 millones de dólares por etiquetar erróneamente el rayón como bambú «sostenible» (Perkins 2023).

Aumento de los riesgos de delincuencia financiera y corrupción

A mayor escala, las empresas que producen desinformación pueden contribuir al aumento de delitos financieros como el blanqueo de capitales, el fraude y la corrupción. La desinformación puede utilizarse para encubrir actividades ilícitas, ocultar la verdadera propiedad de los activos o manipular los informes financieros, todo lo cual puede debilitar los esfuerzos contra el blanqueo de capitales. Por ejemplo, las empresas dedicadas al blanqueo reputacional pueden facilitar u ocultar las actividades de agentes corruptos, de modo que puedan blanquear ganancias ilícitas. Esto no sólo dificulta a los reguladores la detección de delitos financieros, sino que también erosiona la integridad de los sistemas financieros mundiales, aumentando el riesgo sistémico y haciendo que las economías sean más vulnerables a la corrupción y el fraude (Prelec 2022; Wolcott 2022).

Mayor desorden en el entorno informativo

La difusión de desinformación corporativa se suma al creciente problema de la información errónea en el ecosistema de la información en general (Zhou *et al*. 2024). Cuando las empresas contribuyen a crear un entorno en el que la verdad y los hechos son cada vez más difíciles de distinguir de las mentiras y la manipulación, puede erosionarse la confianza del público en los medios de comunicación, las instituciones e incluso los procesos democráticos. El desorden informativo resultante puede tener consecuencias sociales de gran alcance, como el menoscabo de la toma de decisiones fundamentadas, el aumento de la polarización y un debilitamiento general del tejido social. Esta inestabilidad hace más difícil para los reguladores y las instituciones mantener el orden y hacer cumplir las leyes, y contribuye a aumentar la volatilidad del entorno empresarial y político (Colima, Sánchez & Youngs 2021).

Respuesta

Hacer frente a la desinformación corporativa requiere una mezcla de regulación y esfuerzos internos. Los Gobiernos están introduciendo leyes para garantizar que las empresas rindan cuentas por la información engañosa, mientras que muchas empresas están adoptando prácticas para fomentar la transparencia.

Los esfuerzos reguladores de la UE

La Unión Europea se ha situado a la vanguardia de los esfuerzos reguladores para hacer frente a la desinformación, con el Reglamento de Servicios Digitales y el Reglamento de Mercados Digitales como pilares fundamentales de su respuesta. El Reglamento de Servicios Digitales exige que las grandes plataformas de internet mejoren sus prácticas de moderación de contenidos, especialmente la detección y eliminación de contenidos ilegales, como la desinformación. Con ello se obliga claramente a las empresas a garantizar la integridad de sus comunicaciones digitales, ya que ahora se exige que estas plataformas sean más vigilantes a la hora de rastrear y señalar los contenidos corporativos engañosos. Por su parte, el Reglamento de Mercados Digitales pone el foco en la regulación de los grandes guardianes del acceso digital, como las grandes empresas tecnológicas, con el objetivo de evitar que incurran en prácticas desleales como la difusión de desinformación para favorecer sus propios productos o la manipulación de datos de mercado. Al promover la transparencia y una competencia más leal en la esfera digital, el Reglamento de Mercados Digitales pretende limitar el uso de la desinformación como herramienta para obtener beneficios comerciales. En conjunto, esta reglamentación de la UE está diseñada para crear un entorno en línea más seguro y transparente, imponiendo consecuencias legales más estrictas a las empresas que se dediquen a la desinformación o se beneficien de ella (Colima, Sánchez y Youngs 2021).

Regulación más allá de la UE

Fuera de la UE también se han desarrollado respuestas normativas para combatir la desinformación, incluida la corporativa. En Australia, el Código de práctica sobre información errónea y desinformación fomenta la transparencia y la rendición de cuentas estableciendo normas para el tratamiento de la información falsa. Se anima a las empresas a aplicar políticas internas claras para detectar la desinformación y darle respuesta, en particular impartir formación periódica al personal sobre la integridad de la información (Parlamento de Australia 2023).

En Singapur, la Ley de protección contra la falsedad y la manipulación en línea (POFMA) va más allá al permitir que el Gobierno emita órdenes de retirada en caso de desinformación, lo que obliga a las empresas a auditar periódicamente la exactitud de sus comunicaciones y a establecer equipos de respuesta rápida para hacer frente a posibles acciones legales (Zhi Han 2020). En Brasil, la Ley de noticias falsas hace hincapié en la transparencia de las plataformas digitales y recomienda que las empresas mantengan registros detallados de las fuentes de los contenidos que

comparten, de modo que se garantice la rendición de cuentas en casos de difusión de desinformación (De los Santos 2023). En el Reino Unido, el proyecto de Ley de seguridad en línea ofrece orientaciones adicionales e insta a las empresas a adoptar sistemas de moderación de contenidos más estrictos y a colaborar con verificadores independientes para garantizar la rápida detección y eliminación de la desinformación (Departamento de Ciencia, Innovación y Tecnología del Reino Unido 2024).

Gobernanza interna y buenas prácticas en las empresas

Como complemento a las medidas reguladoras, las empresas deben tomar medidas proactivas para reforzar la gobernanza interna y evitar la producción o amplificación de la desinformación. Es esencial realizar auditorías internas periódicas y supervisar el cumplimiento de las estrategias corporativas de comunicación y marketing para detectar los riesgos a tiempo. Los equipos jurídicos y de cumplimiento deben estar facultados para supervisar todos los mensajes públicos a fin de velar por que cumplan las normas legales y sean veraces. La transparencia es clave: las empresas deben compartir abiertamente información sobre sus operaciones, impacto medioambiental y resultados financieros para fomentar la confianza de las partes interesadas. La aplicación de marcos sólidos de responsabilidad social de las empresas (RSE) puede favorecer que estas rindan cuentas conforme a normas éticas, reduciendo la probabilidad de que utilicen el blanqueo reputacional, el blanqueo ecológico u otras prácticas engañosas.

Además, las empresas pueden mejorar la credibilidad de sus comunicaciones colaborando con verificadores independientes o adoptando herramientas de verificación basadas en la cadena de bloques. La tecnología de cadena de bloques, con su registro descentralizado e inmutable, puede utilizarse internamente para garantizar que, una vez registrada la información, permanezca inalterada y a prueba de manipulaciones. Esto ayuda a mantener la integridad de los datos compartidos con el público, proporcionando una capa adicional de verificación que protege contra la manipulación tanto interna como externa (Davison 2024).

Las empresas como blanco de las noticias falsas corporativas

El tercer nexo no sitúa a las empresas como productoras o consumidoras de información errónea o desinformación, sino como blanco de noticias falsas corporativas. Las noticias falsas corporativas pueden ser una forma de información errónea cuando no existe intención de causar daño o engañar, a menudo como resultado de errores honestos o negligencias, por ejemplo, una filtración inexacta del lanzamiento de un producto. Por el contrario, las formas más insidiosas de noticias falsas corporativas —que constituyen desinformación— están diseñadas para engañar y causar daño manipulando la información —por ejemplo, un escándalo fabricado que afecte a un ejecutivo— con el objetivo deliberado de confundir e inducir a error a la

audiencia o a los clientes. Además, las campañas de información maliciosa, que pretenden perjudicar a una empresa sin intención de engañar, consisten en promover noticias reales pero negativas —como la publicación de despidos— para infligir daño a una organización competidora (Park *et al*. 2020: 163).

La amenaza de la información errónea y la desinformación se manifiesta de diversas formas, utilizando distintos medios como texto, audio o vídeo. Los agentes de desinformación pueden crear cuentas falsas en redes sociales, desplegar marketing engañoso en plataformas sociales o motores de búsqueda, o incluso producir contenidos sintéticos, en particular *deepfakes*. La motivación de los ataques de desinformación puede ir desde el beneficio económico y la perturbación de la dinámica competitiva del mercado hasta la incidencia sobre distintas cuestiones (PwC 2022).

El contenido de las noticias falsas corporativas también puede abarcar una serie de temas, como la calidad de los productos, las condiciones laborales y la imagen de marca. Sin embargo, también puede ahondar en cuestiones tales como acusaciones de corrupción, falta de integridad empresarial e incumplimiento de la reglamentación y otras normas de cumplimiento. Un estudio en el que se establecieron categorías de noticias corporativas que afectaban a empresas del índice S&P 500 constató que el 9,9 % de las noticias falsas corporativas estaban relacionadas con *actividades de presión* y presentaban a las empresas afectadas como desleales; el 4,4 % se referían a la *regulación* y caracterizaban a las empresas afectadas como injustas; y alrededor del 1 % se referían a la *corrupción* y calificaban a las empresas afectadas como dañinas (Zhou *et al*. 2024: 5).

En cuanto a las empresas afectadas, el mismo estudio constató que las que tienen mayor visibilidad pública y una cobertura informativa prestigiosa, pero con bajas valoraciones bursátiles, se asocian con mayor frecuencia a noticias falsas. Zhou *et al*. también observaron una correlación positiva entre las bajas valoraciones de los empleados y las noticias falsas centradas en las *actividades de presión* y en la *regulación* (Zhou *et al*. 2024: 7).

En cuanto a la autoría de las noticias falsas, las campañas de información errónea o desinformación pueden ser iniciadas por distintos agentes, como entidades públicas, empresas competidoras o personas oportunistas (PwC 2022). Otro estudio centrado en empresas del índice S&P 500 reveló que las noticias falsas pueden proceder tanto de fuentes externas como internamente de empleados que intentan presionar a la organización. Curiosamente, este estudio no encontró pruebas que apoyaran la idea de que las empresas de sectores altamente competitivos utilizan noticias falsas para difamar a sus rivales (Xu 2021: 13).

Un estudio basado en técnicas de aprendizaje automático ha cartografiado la distribución geográfica de las noticias falsas corporativas y ha descubierto que es probable que se originen fuera del país donde está radicada la sede de la empresa afectada. El estudio también reveló que las noticias falsas corporativas tienden a ser más pronunciadas durante los períodos de mayor tensión geopolítica y es más

probable que afecten a industrias estratégicas y empresas que operan en entornos de información incierta. En el caso de las empresas con sede en Estados Unidos, los países identificados como los mayores difusores de noticias falsas corporativas —según una medida ajustada que compara noticias falsas y reales— fueron Omán, Jordania, Qatar, Marruecos y Líbano (Darendeli, Sun & Peng Tay: 15).

Riesgos

Riesgos reputacionales

Las noticias falsas corporativas presentan importantes amenazas para las empresas, sobre todo en términos de reputación de marca (Castellani & Berton 2017; Mut Camacho 2020; Di Domenico & Visentin 2020; Jahng 2021; Mills & Robson 2019). Un estudio de empresas españolas pone de manifiesto esta preocupación, al revelar que el 98 % de los profesionales percibe la información errónea como una amenaza para la marca, el 86 % la considera un riesgo corporativo y el 80 % ha vivido una crisis provocada por noticias falsas dirigidas contra su empresa (Mut Camacho 2020: 26, 27, 32).

Jahng constata que las empresas afectadas por noticias falsas no relacionadas con la política (por ejemplo, relativas a la calidad del producto) tienen más probabilidades de ser percibidas como enfrentadas a una grave crisis de reputación que las afectadas por noticias falsas relacionadas con la política (por ejemplo, con acusaciones de corrupción o contribuciones políticas ilegales). Esto puede deberse a la creciente sensibilización del público acerca de las motivaciones políticas que subyacen a las noticias falsas y a las diferentes normas de responsabilidad que los consumidores aplican a las empresas frente a los políticos o las instituciones públicas. En consecuencia, los consumidores tienden a pasar por alto las noticias falsas corporativas que tienen motivaciones políticas a la hora de evaluar a una empresa (Jahng 2021: 11).

Sin embargo, las conclusiones de Jahng sobre la crisis de reputación percibida implican que los consumidores son capaces de identificar las noticias falsas relacionadas con la política, lo que resulta cada vez más difícil con el auge de la inteligencia artificial generativa (Saab 2024: 3). Si los consumidores no reconocen que las noticias falsas son efectivamente falsas —ya estén relacionadas con la política, las políticas u otras cuestiones—, la información errónea o la desinformación por motivos políticos podría convertirse en una grave crisis de reputación para las empresas. Un estudio de Public Affairs de 2018 reveló que los estadounidenses consideran las controversias relacionadas con la política y las políticas entre las crisis más graves que puede afrontar una empresa. De todos los escenarios de crisis analizados, las contribuciones ilegales a campañas electorales fueron calificadas como las más graves: un 67 % de los encuestados tenían la opinión más desfavorable de la empresa implicada (Public Affairs 2018: 5). El incumplimiento de las leyes medioambientales también se situó

entre las principales controversias que pueden afectar a una empresa (Public Affairs 2018: 1).

Por ejemplo, JP Morgan experimentó un «choque de información errónea» durante dos meses a finales de 2017, motivado por un escándalo que alegaba que la empresa había transferido 875 millones de dólares a la cuenta de un exministro del petróleo nigeriano, lo que provocó una demanda del Gobierno de Nigeria. A pesar de la sentencia del Tribunal Supremo británico a favor de JP Morgan, la puntuación de la reputación externa de la empresa cayó 2,7 desviaciones estándar (Zhou *et al*. 2024: 9).

Riesgos financieros

Las noticias falsas corporativas también provocan riesgos financieros, que afectan a la cotización bursátil, la manipulación del mercado, la disminución de las ventas y la pérdida de valor de las acciones (Castellani & Berton 2017; Kogan, Moskowitz, & Niessner 2019; Xu 2021; Zhou *et al*. 2024). Según un estudio de la Universidad de Baltimore, la información errónea y la desinformación en línea cuestan a la economía mundial unos 78 000 millones de dólares al año. El estudio constató que la mayor parte de los daños se debieron a pérdidas bursátiles ocasionadas por campañas de desinformación financiera. La proliferación de información errónea también ha hecho que las empresas aumenten el gasto en gestión reputacional, seguridad de marca, salud y bienestar de los empleados y esfuerzos de comunicación de crisis (Cavazos 2019: 13).

Un estudio cuantitativo de empresas del índice S&P 500 documentó una tendencia que demuestra que cuando una empresa se enfrenta a una masa crítica de noticias falsas, en lugar de a un único caso o a un nivel fijo, esta acumulación puede afectar a la reputación externa de la empresa, al estrés laboral interno o incluso a la valoración de sus acciones (Zhou *et al*. 2024: 8). Por ejemplo, los tuits engañosos de Donald Trump causaron importantes pérdidas bursátiles, por ejemplo 1 200 millones de dólares a Toyota tras prometer que impediría que la empresa trasladara sus operaciones a México, donde ya tenía una planta, y 1 000 millones de dólares a Boeing a los pocos minutos de afirmar que los costes de los contratos de la empresa con el Gobierno estaban «fuera de control» (Revesz 2017).

Otro estudio relativo al índice S&P 500 constata que el día que en que aparece una noticia falsa se produce una caída media estadísticamente significativa del 0,18 % de las cotizaciones bursátiles, con una pérdida del 3,1 % del valor de mercado en los tres meses siguientes al suceso. Esta pérdida se eleva al 5,8 % cuando se comparan los rendimientos anómalos acumulados a tres meses de las empresas afectadas con los de empresas fundamentalmente similares pero no afectadas. Curiosamente, el estudio también registró un aumento del volumen de negociación anormalmente positivo en torno a la publicación de noticias falsas, lo que puede reflejar el desacuerdo de los inversores, ya sea debido a diferentes interpretaciones de las noticias o a la exposición selectiva a la información a través de redes en línea segregadas (Xu 2021: 4).

Estas constataciones se corresponden en parte con la investigación sobre artículos falsos de promoción de acciones, que mostró un aumento en el volumen de negociación y un impacto temporal sobre los precios en las empresas más pequeñas, mientras que no se observó tal impacto en las grandes empresas (Kogan, Moskowitz, & Niessner 2019: 43). Existen datos adicionales del sector financiero que permiten estimar que los asesores financieros que suministran información falsa y engañosa cuestan al menos 17 000 millones de dólares en Estados Unidos (Cavazos 2019: 13).

Respuestas

Las respuestas de las empresas a las campañas de desinformación deben tener en cuenta las características particulares de las noticias falsas que las hacen especialmente dañinas. Entre ellas se encuentran la dificultad para identificar la fuente de una noticia falsa, su mayor capacidad de persuasión y la creciente tendencia de los consumidores de información a formarse opiniones basadas en emociones y no en hechos (Mill & Robson 2019: 3). Estas características pueden ser especialmente perjudiciales para las relaciones con clientes muy fieles, ya que la difusión de desinformación puede minar la confianza, un problema que también podía observarse con formas anteriores de información errónea.

Para manejar eficazmente estas amenazas, las empresas deben adoptar un enfoque proactivo, evaluando sus vulnerabilidades específicas, vigilando los canales digitales en busca de señales tempranas de desinformación, fortificando sus marcas corporativas contra posibles ataques y desarrollando planes de recuperación de la información.

Evaluación del riesgo de desinformación

Las empresas pueden establecer estructuras corporativas a través de sus directores de riesgos, directores de seguridad de la información, directores de datos o directores de privacidad, que se enfrentan proactivamente a la desinformación, empezando por evaluar los riesgos informativos específicos a los que se enfrentan. Una evaluación exhaustiva del riesgo de desinformación debe identificar y cuantificar a los principales agentes de desinformación, sus métodos y las amenazas que representan, ya estén relacionadas con beneficios económicos, tácticas competitivas, mensajes políticos o perturbaciones en general (PwC 2022). Además, si una empresa tiene metas y acciones de responsabilidad social corporativa ambiciosas, es esencial que evalúe cuidadosamente su riesgo informativo particular, ya que las tendencias preliminares muestran que las industrias que se centran en cuestiones ambientales, sociales y de gobernanza (ASG) pueden verse más afectadas (Gorham 2023).

Seguimiento y utilización de las redes sociales

Para adelantarse a las campañas de desinformación, es preciso que las empresas vigilen continuamente los canales de las redes sociales. Las empresas pueden participar en el seguimiento y el análisis de opiniones de terceros para calibrar el

discurso público sobre su marca, sus productos y sus empleados. Este seguimiento ofrece dos ventajas fundamentales. En primer lugar, permite alertar en tiempo real a la empresa y al equipo de crisis tras la detección de conversaciones o artículos de importancia crítica. En segundo lugar, facilita el análisis en profundidad del alcance y el impacto de la crisis en toda la red (Adriani 2022).

Las empresas deberían considerar la posibilidad de asociarse con consultores externos especializados en revisar las redes sociales en busca de palabras clave de desinformación y menciones injustificadas del nombre de la empresa. Las empresas también pueden evaluar el uso de herramientas de automatización que utilizan la IA y el aprendizaje automático para escanear plataformas de redes sociales en busca de información falsificada, o empresas que evalúen datos no estructurados, como manipulaciones de audio y vídeo (Bank of America 2023a: 5)

Además, es crucial identificar a personas influyentes que puedan difundir desinformación. Saber quiénes son, quiénes les apoyan y su ubicación geográfica permite a las empresas anticiparse a las posibles amenazas y mitigarlas. Si una persona influyente no es consciente de que la información es inexacta, la empresa puede intentar cultivar la relación con ella. Crear una comunidad de defensores y fomentar una narrativa positiva en torno a la marca permite a las empresas combatir la desinformación con mayor eficacia antes de que gane terreno (PwC 2022).

Información contra la desinformación

Las empresas deben fortalecer sus marcas contra la desinformación mediante una comunicación continua y auténtica con sus clientes, tanto a través de los canales digitales como de los tradicionales. La acción proactiva ayuda a las empresas a evitar los riesgos de verse sorprendidas con la guardia baja o tener que responder a la defensiva (PwC 2022). Cuando aparece una información negativa, es más probable que los clientes pidan aclaraciones directamente a la empresa, por lo que las organizaciones deben estar preparadas para actuar con rapidez en respuesta a la desinformación. Una de las estrategias más consolidadas que pueden emplear las empresas es revelar información como respuesta de refutación. Revelar información es un instrumento eficaz para corregir las percepciones erróneas, mitigar los daños y restablecer la reputación (Chakravarthy *et al*. 2014; Lee *et al*. 2015).

Los estudios también indican que, si bien la información errónea y la desinformación sobre las empresas han motivado en efecto que se tomaran decisiones estratégicas de revelación de información en los últimos años (Langberg & Sivaramakrishnan 2008; Baloria & Heese 2018; Frenkel *et al*. 2020), no siempre es así. Un estudio cuantitativo descubrió que las empresas responden voluntariamente solo al 20 % de las noticias falsas corporativas dirigidas contra ellas (Xu 2021). Puede que las empresas duden en responder creyendo que los inversores racionales no se dejarán influir por la información errónea, o que una respuesta podría conferir credibilidad a las afirmaciones falsas sin pretenderlo. Sin embargo, el mismo estudio revela que las empresas que responden a las noticias falsas reducen la probabilidad de futuros

ataques aproximadamente en un 19 %. Además, las empresas que actúan con rapidez —tardan menos días en responder— reducen significativamente el impacto negativo acumulado de las noticias falsas en la rentabilidad de sus acciones (Xu 2021: 17).

Para contrarrestar la desinformación, las empresas pueden participar en diversas iniciativas que promuevan fuentes de confianza y faciliten el acceso a medios de comunicación fidedignos. La coalición Ads for News, liderada por Internews, anima a las marcas a anunciarse directamente en medios de comunicación reputados, apoyando así el periodismo de calidad. Del mismo modo, Trusted Media, establecida por DPG Media en los Países Bajos, conecta a los anunciantes con fuentes de noticias fiables. La Journalism Trust Initiative ayuda a identificar proveedores de noticias creíbles para los anunciantes, mientras que el Check My Ads Institute exige a empresas de tecnología publicitaria como Google y Meta que rindan cuentas por los contenidos que promocionan. En el Reino Unido, el Ozone Project —una colaboración entre News UK, Telegraph Media Group y Guardian News and Media— ofrece una plataforma publicitaria que dirige a los anunciantes a entornos de calidad a través de un único punto de compra. Esta iniciativa declaró haber llegado a 41,1 millones de consumidores en 2018, igualando el tamaño de la audiencia de Facebook y Google. Además, en Italia, CityNews, una red de medios locales que cubre 53 ciudades, consiguió aumentar sus ingresos publicitarios en un 7 % dando prioridad a la publicidad local, que suele ser más resiliente que la nacional (Brogi & Sjøvaag 2023: 23). Al participar en estas iniciativas, las empresas pueden reforzar su compromiso de contrarrestar la desinformación y promover un panorama mediático más saludable.

Elaboración de un plan de recuperación frente a la desinformación

Aunque las soluciones para prevenir o mitigar la información errónea o la desinformación pueden ser limitadas, las empresas deben poner el foco en las técnicas de respuesta y desarrollar un plan de recuperación frente a la desinformación en consonancia con sus estrategias existentes de gestión de incidentes y crisis. Este plan debe implicar la creación de todo un manual de estrategia que describa los protocolos de respuesta a los ataques de desinformación, y debe ponerse a prueba periódicamente mediante simulaciones y ejercicios (PwC 2022). El análisis de las partes interesadas es un componente clave, ya que identifica a los grupos con los que hay que comunicarse durante un acto de desinformación y garantiza una clara rendición de cuentas y la difusión del mensaje. Las empresas también deben elaborar narrativas adaptadas a los distintos tipos de ataque y centradas en cuestiones específicas de su sector o ubicación geográfica. Por último, es fundamental establecer un sistema que mida la eficacia de la respuesta a la desinformación, lo que permitirá a las empresas aprender de cada incidente y prepararse mejor para futuras amenazas.

References

Adriani, R. 2022. Fake News Versus Corporate Reputation: Techniques to Protect Brands. International Journal of Social Sciences, 8(1), 121–137.

Albisu, I. 2020. Experiences of compliance reviews by CSOs: Lessons learned and challenges. Transparency International Anti-Corruption Desk.

Allcott, H. & Gentzkow, M. 2017. Social media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), 211-36.

Aïmeur, E., Amri, S. & Brassard, G. 2023. Fake news, disinformation and misinformation in social media: a review. Social Network Analysis and Mining (2023) 13:30.

Anderson, J. & Gray, C. 2006. Anti-Corruption in Transition 3: Who is Succeeding ... and why? The World Bank.

Athanasouli, D., Goujard, A. & Sklia, P. 2012. Corruption and Firm Performance: Evidence from Greek Firms. International Journal of Economic Sciences and Applied Research, Vol. 5 No.1, pp. 43–67.

Baloria, V.P., & Heese, J. 2018. The effects of media slant on firm behaviour. Journal of Financial Economics 129, 184-202.

Bank of America. 2023. The threat misinformation and disinformation pose to business. Cyber Security Journal Issue 7.

Bbaale, E. & Okumu, I.M. 2018. Corruption and firm-level productivity: greasing or sanding effect? World Journal of Entrepreneurship, Management and Sustainable Development, Vol. 14.

Bennet, L.W. & Livingston, S. 2018. The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication, 33(2), 122-139.

Bennet, L.W. & Uldam, J. 2024. *Corporate Social Responsibility in The Disinformation Age*. Management Communication Quarterly, 0(0).

Bitiukova, N., Bayer, J., Bard, P., Szakacs, J., Alemanno, A., Uszkiewicz. 2019. Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States. Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union.

Bonneuil, C., Choquet, P.L. & Franta, B. 2021. Early warnings and emerging accountability: Total's responses to global warming, 1971–2021. Global Environmental Change, Volume 71.

Bontcheva, K., & Posetti, J. (eds.). 2020. Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression, UNESCO Broadband Commission Report.

Brennan, M. 2023. Media Confidence in U.S. Matches 2016 Record Low. Gallup News Politics.

Brogi, E. & Sjøvaag, H. 2023. Good practices for sustainable news media financing Prepared by the Committee of experts on increasing resilience of media (MSI-RES). Council of Europe.

Burki, T. 2020. The online anti-vaccine movement in the age of COVID-19. The Lancet, volume 2 (10).

Cahill, S. 2017. 2017. Imagining alternatives in the Emerald City: the climate change discourse of transnational fossil fuel corporations. University of Victoria.

Caramancion, K.M. 2020. An Exploration of Disinformation as a Cybersecurity Threat. 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, pp. 440-444

Carr, C. T. & Hayes, R. 2015. Social media: Defining, Developing, and Divining. Atlantic Journal of Communication, 23(1), 46–65.

Castellani, P. & Berton, M. 2017. Fake news and corporate reputation: What strategies do companies adopt against false information in the media? 20th Excellence in International Conference Services, University of Verona.

Cavazos, R. The Economic Cost of Bad Actors on the Internet: Fake News in 2019. University of Baltimore & CHEQ.

Chakravarthy, J., deHaan, E. & Rajgopal, S. 2014. Reputation repair after a serious restatement. The Accounting Review 89, 1329-1363.

Coan, T.G., Boussalis, C., Cook, J. & Nanko, M.O. 2021. Computer-assisted classification of contrarian claims about climate change. Sci Rep;11(1).

Colima, C., Sanchez, H.& Youngs, R. 2021. The impact of disinformation on democratic processes and human rights in the world. European Parliament: Policy Department for External Relations. Directorate General for External Policies of the Union PE 653.635 - April 2021.

Cook, J., Lewandowsky, S., Ecker, U.K.H. 2017. Neutralizing misinformation through inoculation: Exposing misleading argumentation techniques reduces their influence. PLoS One. 2017 May 5;12(5).

Cook, J., Supran, G., Lewandowsky, S., Oreskes, N., & Maibach, E. 2019. America Misled: How the fossil fuel industry deliberately misled Americans about climate change. Fairfax, VA: George Mason University Center for Climate Change Communication.

Council of the European Union. 2024. Combatting corruption: Council adopts position on EU law. Press Releases, Council of the European Union.

Dai, J., Wang, Y. & Vasarhelyi, M.A. 2017. Blockchain: An Emerging Solution for Fraud Prevention. The CPA Journal, Vol.87(6), pp.12-14.

Darendeli, A., Sun, A. & Peng Tay, W. The geography of corporate fake news. PLoS ONE 19(4): e0301364.

Davison, T. 2024. Greenwashing Examples: The Nine Biggest Fines Handed Out So Far. Clean Hub.

Davison, T. 2024. Top 9 Ways to Avoid Greenwashing in Your Business. Clean Hub.

De los Santos, B. 2023. Fake News Bill: understand in 6 points the legislation being discussed in Congress. Conectas Human Rights.

De Rosa, D., Gooroochurn, N. & Görg, H. 2015. Corruption and Productivity: Firm-level Evidence. Jahrbücher für Nationalökonomie und Statistik. Vol. 235, no. 2, pp. 115-138.

De Freitas Netto, S.V. et al. 2020. *Concepts and forms of greenwashing: a systematic review*. Environmental Sciences Europe 32, 19.

Dunlap, R. & McCright, A. 2011. Organized Climate denial in The Oxford Handbook of Climate Change and Society. Oxford University Press.

Dutta, N. & Sobel, R. 2016. Does corruption ever help entrepreneurship? Small Bus Econ 47, 179–199.

Ecker, U.K.H., Lewandowsky, S., Cook, J. et al. 2022. The psychological drivers of misinformation belief and its resistance to correction. Nat Rev Psychol 1, 13–29.

EU vs Disinfo. 2017. DISINFO: Emmanuel Macron's campaign has been funded by Saudi Arabia. Disinformation database entry.

Fletcher, R. 2020. Trust Will Get Worse Before It Gets Better. Oxford: Reuters Institute for the Study of Journalism.

Franta, B. 2021. Early oil industry disinformation on global warming. Environmental Politics, Volume 30 (4).

Frenkel, S., Guttman, I., Kremer, I. 2020. The effect of exogenous information on voluntary disclosure and market quality. Journal of Financial Economics 138, 176-192.

Gorham, M. 2023. Disinformation: a guide to understanding and mitigating the risks to your business. Global strategy and international business insights, Judge Business School, University of Cambridge.

Hanley-Giersch, J. & Brokes, F. 2024. The Rise of Disinformation in OSINT. Berlin Risk Blogpost.

Henriks, W. 2022. Disinformation and the First Amendment: Fraud on the Public. St. John's L. Rev. (96) pp. 543-589.

Ho, Charlyn. 2024. AI And Blockchain Can Mitigate Fraud Risk Caused by Deepfakes. Forbes.

Hotten, R. 2015. Volkswagen: The scandal explained. BBC News.

Innes, H., Innes, M. & Dawson, A. 2023. OSINT vs Disinformation: The Information Threats 'Arms Race'. Crest Cybersecurity Review.

Institute for Financial Integrity. 2024. The Importance of Media in Due Diligence. Blogpost.

Jahng, M.R. 2021. Is Fake News the New Social Media Crisis? Examining the Public Evaluation of Crisis Management for Corporate Organizations Targeted in Fake News. International Journal of Strategic Communication.

Jagemast, H. 2023. Flood disaster in Libya: Fake news to cover up corruption. Dis: orient Magazine.

Jenkins, M. 2018. The relationship between business integrity and commercial success. Transparency International Anti-Corruption Desk.

Jones, K. 2019. Online Disinformation and Political Discourse Applying a Human Rights Framework. Chatham House, The Royal Institute of International Affairs.

Jurkowitz, M., Mitchell, A., Shearer, E. & Walker, M. 2020. U.S. Media Polarization and the 2020 Election: A Nation Divided. Washington, DC: Pew Research Center.

Karpoff, J.M., Lee, S. &Martin, G.S. 2012. The Impact of Anti-Bribery Enforcement Actions on Targeted Firms. SSRN Electronic Journal.

Khavanov, A. 2024. Utilizing OSINT for Enhanced Anti-Corruption Compliance in Third-Party Due Diligence.

Kemsley, H., Corbett, S. & Cooke, D. 2024. Mis/Disinformation in Open-Source Intelligence. Janes.

Kogan, S., Moskowitz, T.J. & Niessner, M. 2018. Social media and Financial News Manipulation. SSRN.

Kossow, N. 2018. Fake news and anti-corruption. Transparency International Anti-Corruption Helpdesk Answer.

Lamb, W.F., Mattioli, G., Levi, S. et al. 2020. Discourses of climate delay. Global Sustainability. 2020;3: e17.

Langberg, N., & Sivaramakrishnan, K. 2008. Voluntary disclosures and information production by analysts. Journal of Accounting and Economics, 46, 78-100.

Laufer, W.2003. Social Accountability and Corporate Greenwashing. Journal of Business Ethics 43, 253–261.

Lee, L.F., Hutton, A.P., Shu, S. 2015. The role of social media in the capital market: Evidence from consumer product recalls. Journal of Accounting Research 53, 367-404.

Leighton, N. 2023. Marketing Misinformation: A Thin Line Between Persuasion and Deception. Forbes.

Lescher, G. 2022. Fake sustainability harbours risks: Greenwashing. PwC.

Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. 2012. Misinformation and Its Correction: Continued Influence and Successful Debiasing. Psychological Science in the Public Interest, 13(3), 106-131.

Martins, L., Cerdeira, J. & Teixeira, A. 2020. Does corruption boost or harm firms' performance in developing and emerging economies? A firm-level study. The World Economy, Volume 43 (8).

Mason, C. & Oxnevad, I. 2024. The AI-Disinformation Threat to Companies. Corporate Compliance Insights.

McClimon, T.J. 2022. Bluewashing Joins Greenwashing as The New Corporate Whitewishing. Forbes.

Medeiros, P. et al. 2024. Greenwashing and Disinformation: Brazilian Agribusiness' Toxic Advertising on Social Media. Publicidade e Desenvolvimento Sustentável (45).

Megerisi, T. 2023. Libyan Floods Reflect a River of Corruption and Negligence. New Lines Magazine.

Mills, A. J. & Robson, K. 2019. Brand management in the era of fake news: narrative response as a strategy to insulate brand value. Journal of Product & Brand Management, JPBM-12-2018-2150.

Mohan, M. 2017. Macron Leaks: the anatomy of a hack. BBC News.

Mut Camacho, M. 2020. Learning about reputational risk in the era of Covid-19: disinformation as corporate risk. Doxa Comunicación, 31, pp. 19-39.

Naderer, B., Schmuck, D. & Matthes, J. 2017. Greenwashing: Disinformation through Green Advertising. In Commercial Communication in the Digital Age: Information or Disinformation? edited by Siegert, G., Rimscha, B. & Grubenmann, S. Berlin, Boston: De Gruyter Saur, 2017, pp. 105-120.

National Agency on Corruption Prevention Ukraine. 2024. Corruption is in the focus of Kremlin's information operations against Ukraine: results of a research of disinformation narratives.

Nichols, P.M. 2012. The Business Case for Complying with Bribery Laws. American Business Law Journal. Vol. 49(2), pp 325-368.

Nisbet, M.C. 2009. Knowledge Into Action: Framing the Debates Over Climate Change and Poverty. In Doing News Framing Analysis: Empirical and Theoretical Perspectives. Routledge.

Newman, N., Fletcher, R., Schulz, A., Andi, S., & Nielsen, R. K. 2020. Reuters Institute Digital News Report 2020. Oxford: Reuters Institute for the Study of Journalism.

OECD. 2014. OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials. OECD Publishing, Paris.

OECD. 2024. The OECD Truth Quest Survey: Methodology and Findings. OECD Publishing, Paris.

Organization for Security and Co-operation in Europe. 2017. Joint declaration on freedom of expression and "fake news", disinformation and propaganda.

Ognyanova, K., Lazer, D., Robertson, R. E., & Wilson, C. 2020. Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. The Harvard Kennedy School (HKS) Misinformation Review, Volume 1, Issue 4.

Park, A., Montecchi, M., Plangger, K., Pitt, L. et al. 2020. Understanding fake news: a bibliographic perspective. Defense Strategic Communications, 8 (Spring 2020): 141–172.

Parliamentary Assembly of the Council of Europe. 2020. Democracy hacked? How to respond?

Parliament of Australia. 2023. Media literacy and misinformation. Communications and Media.

Pennycook, G. & Rand, D.G. 2021. The Psychology of Fake News. Trends Cogn Sci. May;25(5):388-402.

Perkins, T. 2023. A sea of misinformation: FTC to address industry greenwashing complaints. The Guardian.

Petratos, P.N. & Faccia, A. 2023. Fake news, misinformation, disinformation and supply chain risks and disruptions: risk management and resilience using blockchain. *Ann Oper Res* 327, 735–762.

Prelec, T. The Magic Wand of Reputation Laundering: Turning Kleptocrats into "Engaged Global Citizens". Global Insights.

Public Affairs Council. 2018. Fight or Flight: How Americans React to Corporate Crises and Controversies. Public Affairs Council and Morning Consult.

PwC.2022. Disinformation attacks have arrived in the corporate sector. Are you ready? Cybersecurity, PwC US.

Randhawa, A. et al. 2023. Thoughts on the new Economic Crime and Corporate Transparency Act - A New Era for Corporate Criminal Liability in the UK. White & Case Insight Alerts.

Saab, B. 2024.Manufacturing Deceit: How Generative AI Supercharges information manipulation. National Endowment for Democracy and International Forum for Democratic Studies Report.

Schneider, J., Schwarze, S., Bsumek, P. & Peeples, J. 2016. Under Pressure: Coal Industry Rhetoric and Neoliberalism. Palgrave Macmillan.

Seelow, S. 2017. Champs-Elysées attack: the murky role of social networks. Le Mond.

Serafeim, G. 2014. Firm Competitiveness and Detection of Bribery. Harvard Business School Working Paper, No. 14-012.

Supran, G & Oreskes, N. 2021. Rhetoric and frame analysis of ExxonMobil's climate change communications. One Earth, volume 4 (5).

Supran, G & Hickey, C. 2022. Three Shades of Green(washing): Content Analysis of Social Media Discourse by European Oil, Car, and Airline Companies. Algorithmic Transparency Institute & Harvard University.

Transparency International. 2015. Anti - Corruption Glossary: Compliance.

Teichmann, F., Ruxandra, S. & Sergei, B. 2022. International management amid fake news and corruption. Journal of Financial Crime 30(34).

Toff, B. et al.2020. What We Think We Know and What We Want to Know: Perspectives on Trust in News in a Changing World. Reuters Institute for the Study of Journalism.

UK House of Commons Select Committee on Digital, Culture, Media and Sport. 2019. Disinformation and 'Fake News': Final Report.

UK Department for Science, Innovation and Technology. 2024. Online Safety Act: explainer. Guidance.

Union of Concerned Scientists. 2007. Smoke, Mirrors & Hot Air: How ExxonMobil Uses Big Tobacco's Tactics to Manufacture Uncertainty on Climate Science.

UNODC. 2013. An Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide. United Nations Office on Drugs and Crime.

US Department of Justice. 2017. Volkswagen AG Agrees to Plead Guilty and Pay $4.3 Billion in Criminal and Civil Penalties; Six Volkswagen Executives and Employees are Indicted in Connection with Conspiracy to Cheat U.S. Emissions Tests. U.S. Department of Justice Criminal Division, Press Release.

US Department of Justice. 2023. Evaluation of Corporate Compliance Programs. U.S. Department of Justice Criminal Division.

Van Vu, H., Tran, T.Q., Van Nguyen, T. et al. 2018. Corruption, Types of Corruption and Firm Financial Performance: New Evidence from a Transitional Economy. J Bus Ethics 148, 847–858.

Vosoughi, S., Roy, D., Aral, S. 2018. The spread of true and false news online. MIT Initiative on the Digital Economy Research Brief.

Wang, Y. 2021. Research on Impacts of Bribery on Different Business Sectors. Advances in Economics, Business and Management Research, volume 203 Proceedings of the 2021 3rd International Conference on Economic Management and Cultural Industry.

Wegner, S., Schöberlein, J. & Biermann, S. 2013. Motivating Business to Counter Corruption A Practitioner Handbook on Anti-Corruption Incentives and Sanctions. Humboldt-Viadrina School of Governance.

Wihbey, J. 2014. The Challenges of Democratizing News and Information: Examining Data on Social Media, Viral Patterns and Digital Influence. Politics and Public Policy Discussion Paper Series: #D-85. Shorenstein Centre on Media, Harvard Kennedy School.

Williams, E., Bartone, S., Swanson E.K. & Stokes, L.C. 2022. The American electric utility industry's role in promoting climate denial, doubt, and delay. Environmental Research Letters (17).

Wolcott, R. 2022. Reputation launderers,' disinformation campaigns hinder sanctions and financial crime compliance efforts. Thomson Reuters.

Xu, R. 2021. *Corporate Fake News on Social Media*. Ph.D. thesis, University of Miami.

Zhi Han, T. 2020. Protection from Online Falsehoods and Manipulation Act (POFMA): Regulating Fake News to Maintain Public Trust in Singapore. Konrad Adenauer Foundation.

Zhou, K., Scepanovi, S., Quercia, D. 2024. Characterizing Fake News Targeting Corporations. Proceedings of the Eighteenth International AAAI Conference on Web and Social Media (ICWSM 2024).

Transparency International
International Secretariat
Alt-Moabit 96
10559 Berlin
Germany

Phone: +49 - 30 - 34 38 200
Fax: +49 - 30 - 34 70 39 12

tihelpdesk@transparency.org
www.transparency.org

transparency.org/en/blog
facebook.com/transparencyinternational
twitter.com/anticorruption