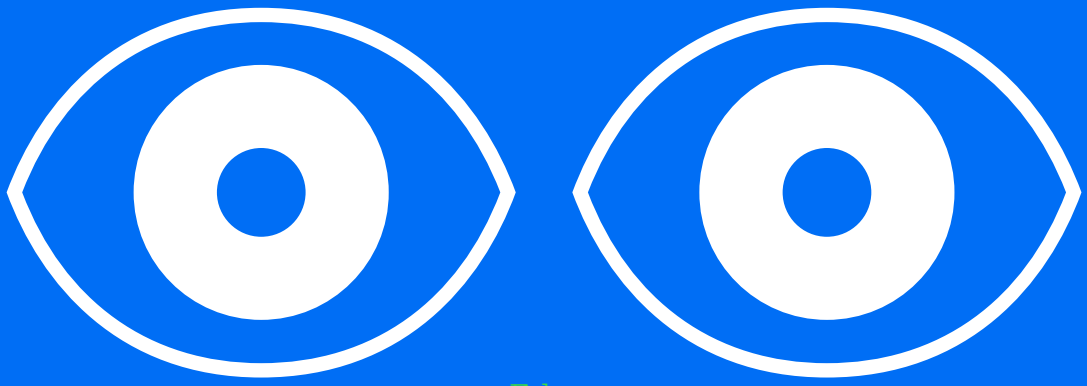
# Contra la desinformación:

## Manual de herramientas y recursos didácticos para el aula



Eds.
José Rúas Araújo
Julia Fontenla Pedreira

EDITORIAL fragua

# Contra la desinformación:

Manual de herramientas y recursos didácticos para el aula

EDITORIAL Fragua

Director de la Colección:
**Ignacio Muñoz Maestre**

Título:
**Contra la desinformación: Manual de herramientas y recursos didácticos para el aula.**

Diseño y Maquetación:
**Xurxo Baca + Gerardo Covela**

**© EDITORIAL FRAGUA**
C/. Andrés Mellado, 64. 28015, Madrid
Tel. 915-491-806/ 915-442-297
E-mail: editorial@fragua.es
www.fragua.es

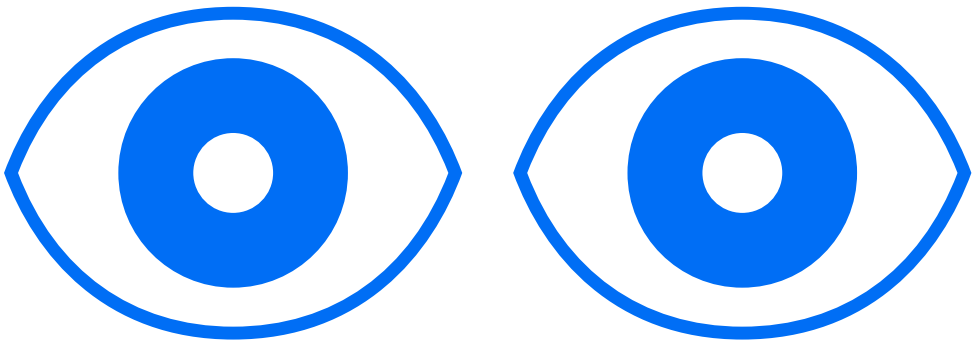
**I.S.B.N.: 978-84-7074-739-7** (pdf)

Este Manual forma parte de las actividades promovidas a través del proyecto "Lucha contra la desinformación y los estándares de valor en los debates electorales en TV y medios digitales: plataforma de verificación y blockchain (DEBATrue)", con Ref. PDC2021-121720-100, del Programa Estatal de I+D+i para la realización de Pruebas de Concepto, del Programa Estatal Retos de la Sociedad, Programa Estatal de Investigación Científica, Técnica y de Innovación 2017-2020.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA E INNOVACIÓN · AGENCIA ESTATAL DE INVESTIGACIÓN

Plan de Recuperación, Transformación y Resiliencia



Aquí tienes un *Manual contra la Desinformación,* con herramientas y recursos didácticos para el aula, dirigido al alumnado y profesorado de Secundaria y Bachillerato. Confiamos en que os sirva de ayuda en vuestros centros escolares, para entender mejor el fenómeno de la desinformación y las noticias falsas y a observarlo con perspectiva, con la intención de animaros a la discusión y el debate crítico.

Contamos para ello con la aportación de profesores y académicos expertos en distintos ámbitos, desde la comunicación, el marketing y la economía, la filosofía, la sociología, el derecho, la informática y la defensa, que trabajan como profesionales e investigadores en diversos proyectos relacionados con la lucha contra la desinformación y que aportaron sus conocimientos, en este Manual que ponemos a vuestra disposición, con la ayuda del Ministerio de Ciencia e Innovación.

# índice

# 8

# ¿eres alternativo? pues explora la internet independiente

Alberto Quian

***ALBERTO QUIAN*** *es Doctor en Investigación en Medios de Comunicación y Premio Extraordinario de Doctorado por la Universidad Carlos III de Madrid. Profesor de Periodismo en la Facultad de Ciencias de la Comunicación de la Universidade de Santiago de Compostela. Su principal línea de investigación se centra en el impacto y la aplicación de la cultura y ética hackers en el periodismo, los medios de comunicación y las redes sociales.*

alberto.quian@usc.es

## resumen

La web fue un regalo de Tim Berners-Lee a la humanidad para navegar de manera sencilla por Internet y democratizar su uso. La idea primigenia fue crear una web descentralizada y abierta. Pero las grandes tecnológicas y gobiernos se han apoderado de ella para centralizarla y crear un sistema de vigilancia y control global. Frente a esto, cada vez más personas están migrando a la Internet alternativa e independiente, donde la soberanía de los datos y algorítmica reside en los usuarios, la privacidad es un derecho fundamental y la información fluye libremente, sin censura. Los espacios de la Internet alternativa no están libres de desinformación, pero por su naturaleza parecen más resistentes a la manipulación. En este capítulo se presentan algunos sistemas y herramientas con los que explorar esa Internet independiente y libre: desde navegadores como TOR o buscadores como DuckDuckGo, hasta protocolos como Gemini, los grupos de noticias de Usenet y las redes sociales del Fediverso.

# 01. Introducción

Los algoritmos nos condicionan en Internet. Nos recomiendan noticias, música, películas, ropa, libros, restaurantes, bares y discotecas, viajes, usuarios de redes a los que seguir, incluso personas que podrían ser el amor de nuestra vida. Los algoritmos nos incitan a hacer cosas que nos pueden gustar basándose en nuestros datos y cruzándolos con los de otros internautas con comportamientos similares o con los que interactuamos de una forma u otra en la red (Reviglio y Agosti, 2020). Tu fecha de nacimiento, tu origen, tu lugar de residencia, tus creencias, tu ideología política, tus estudios, tu profesión, tus aficiones, tus compras, tus amistades en redes sociales, tus amores, tus movimientos geolocalizados, tus clics en Internet..., todo se registra y se analiza para alimentar a los algoritmos de las plataformas y servicios de las grandes compañías tecnológicas: Google, Meta, X (Twitter), Amazon, Apple, Microsoft... Nada se les escapa en la «economía de la vigilancia» o «capitalismo de vigilancia» (Véliz, 2021; Zuboff, 2020). Recolectan, cruzan, analizan y venden nuestros datos para generar un inmenso negocio (Dhawan et al., 2022).

En este contexto, la desinformación se ha mostrado muy rentable. Tenemos datos que demuestran que la mentira se expande más rápido y vende más que la verdad (Vosoughi, Roy y Aral, 2018). Algunas campañas de informaciones falsas han sido potenciadas por algoritmos de las «big tech». Un ejemplo: el escándalo de la empresa Cambridge Analytica (Kaiser, 2019) nos mostró cómo los mercenarios de la desinformación actuaron en 2016 en la campaña de las elecciones presidenciales en Estados Unidos, que ganó el populista y ultraderechista Donald Trump, y en la del referéndum en Reino Unido que supuso su salida de la Unión Europea («Brexit»), patrocinada también por fuerzas populistas y ultraderechistas. Aquellas campañas, basadas en mentiras y mensajes de odio, y propulsadas por algoritmos, marcaron el inicio de la era de la posverdad (d'Ancona, 2019; Ferraris, 2019; McIntyre, 2018).

Ningún rincón de la Red está libre de ser intoxicado por informaciones falsas, contenidos engañosos y discursos de odio. Pero sí hay espacios donde se pueden minimizar los riegos y herramientas para reducir la exposición a estos o frenarlos, además de garantizarte una experiencia más segura para tu privacidad y la «soberanía algorítmica» (Reviglio y Agosti, 2020).

Lo que aquí te propongo es una aventura por algunos de los muchos espacios y herramientas de la Red alternativa bajo el paraguas de la ética hacker, la cual fundamentalmente defiende de la libertad de expresión, la información y la cultura libres, el acceso universal al conocimiento, el derecho a la privacidad, la transparencia gubernamental y corporativa, y la descentralización de Internet (Quian, 2022), esto es, que la Red y nuestros datos no sean controlados por compañías y gobiernos (Snowden, 2019).

## 02. Los riesgos de googlear

Los motores de búsqueda son una de las principales vías de acceso a la información y a productos y servicios en Internet. Pero sabemos que son también ventiladores de desinformación a escala global, posicionando entre los resultados destacados contenidos sensacionalistas, teorías de la conspiración, noticias falsas, mensajes de odio, informaciones sesgadas y todo tipo de consejos de seudoexpertos (Bradshaw, 2019; Shah, 2021). Diseñados por especialistas en SEO (Search Engine Optimization) y SEM (Search Engine Marketing) y alimentados por algoritmos que aprenden de nuestras búsquedas y clics, estos contenidos se han convertido en un lucrativo negocio (Hoffmann, Taylor y Bradshaw, 2019) y en una amenaza a escala mundial para la salud pública, el conocimiento, la verdad histórica, los derechos humanos y nuestras libertades.

Buscar información sobre cualquier cosa en Internet es de lo más simple y rutinario que hacemos a diario. Pero dónde y cómo lo hagamos puede tener consecuencias diferentes. Un consejo que doy a mis alumnos es que no hagan búsquedas en Google sobre problemas de salud personales. Parece una tontería, pero no lo es. Cada vez que accedes a Google, tu ip (es como tu dirección postal en Internet) y todas tus acciones quedan registradas. Esas búsquedas las harás, muy probablemente, desde una cuenta personal de Google en la que has introducido datos personales para usar también otros servicios de la compañía Alphabet (Google Chrome, Gmail, YouTube, Google Calendar, Google Maps, etc.), en los que también queda registrada tu actividad. Y todos esos datos y acciones se cruzarán con los de otros usuarios y se compartirán con los de otras compañías y afiliados para hacer negocio. Por eso, cuando compras algo por Internet, o ves una película en una plataforma de streaming, o visitas recurrentemente un portal de información, o visualizas determinados vídeos en YouTube, verás que Google lo sabe porque te mostrará, mediante publicidad, recomendaciones o resultados de búsqueda, informaciones, productos y servicios iguales o relacionados con lo que consumes. De igual modo, cada vez que haces en Google una búsqueda tipo «tengo un bulto en el pecho, ¿qué hago?», estás transfiriendo a esta compañía información personal, privada, sobre tu salud con la que podrá traficar con terceros para ofrecerte campañas publicitarias y resultados de búsqueda de sitios web que pagan y utilizan estrategias para posicionarse en los primeros puestos de Google o en los contenidos destacados y recomendados de YouTube o de Google Discover, por ejemplo. Muchos son fuentes poco o nada confiables, factorías de desinformación sin aval científico-médico.

Un par de ejemplos. Un análisis de vídeos en YouTube sobre la covid-19 mostró que algo más de una cuarta parte de los más vistos contenía información engañosa vista por decenas de millones de personas (Li et al., 2020). Otro estudio similar, pero sobre vídeos en los que se habla de cáncer de mama, reve-

ló que poco más de un 18% eran de expertos y una cuarta parte no ofrecía información fiable; es más, los vídeos creados por no expertos tenían más visualizaciones (Míguez González, García Crespo y Ramahí García, 2020). Así que si buscas en Google «me ha salido un bulto en el pecho, ¿qué hago?», es probable que te sugiera algunos de esos vídeos poco o nada fiables, pero más populares, o páginas web con contenidos no revisados por especialistas.

Esto no solo funciona en los servicios de Alphabet, también sucede en los de otras «big tech», como Meta (Instagram, Facebook, WhatsApp...), X (Twitter), ByteDance (TikTok, Toutiao...), Amazon (tienda Amazon, Twitch, Goodreads, IMDb...) o Microsoft (Twitch, Bing, Edge...), entre otras, donde los algoritmos gobiernan nuestra atención, encerrándonos en filtros burbuja (Pariser, 2017).

**Figura 1. Campaña de la organización La Quadrature du Net contra las GAFAM (Google, Apple, Facebook, Amazon y Microsoft)**


Fuente: GAFAM poster campaign https://gafam.info/

Pero Google es un caso paradigmático. En agosto de 2023 controlaba el 64,66 % de la cuota de mercado de navegadores móviles en el mundo, el 63,56 % de navegadores de escritorio, los sistemas operativos del 70,76 % de los dispositivos móviles y el 91,85 % de las búsquedas en internet, según datos de StatCoun-

ter (sitio de análisis de tráfico web): Su dominio es apabullante; su poder, descomunal: https://gs.statcounter.com/

Entonces, ¿qué podemos hacer? Escapar... sin desconectarnos. Existen muchas maneras de hacerlo.

## 03. Cómo escapar de Google

Buscar en Google, utilizar su navegador Chrome, ver vídeos en YouTube, usar el correo electrónico de Gmail o desplazarnos con la ayuda de Google Maps tiene algunas ventajas, fundamentalmente, que son servicios integrados, fáciles de usar, útiles y populares. Pero vivir fuera de Google y de las herramientas y plataformas interconectadas que controla Alphabet es posible y puede ser más seguro para tu privacidad y, por lo tanto, también para tu manera de consumir información, acceder a contenidos, adquirir productos y servicios, o interactuar con otras personas. Existen numerosas alternativas; aquí te explico algunas.

**Figura 2. Campaña de la organización La Quadrature du Net contra las GAFAM (Google, Apple, Facebook, Amazon y Microsoft)**


Fuente: GAFAM poster campaign https://gafam.info/

## 3.1. Navega seguro con TOR y los servicios cebolla

El proyecto sin ánimo de lucro TOR (The Onion Router - https://www.torproject.org/) aplica tecnología criptográfica para una navegación anónima y segura, protegiendo tu privacidad. Su navegador (software libre y de código abierto) disfraza tu dirección real en la Red (IP) e impide que tu proveedor de servicios de internet (ISP) y otros agentes que puedan estar observando tu conexión rastreen tu actividad, incluyendo los sitios web que visites. TOR también evita que los sitios web realicen «fingerprinting» (patrones de comportamiento de usuarios) o te identifiquen por la configuración de tu navegador. Otra ventaja es que no conserva ningún historial de navegación y las cookies sólo son válidas durante una sola sesión.

TOR es una red de túneles virtuales. Lo que hace, básicamente, es cifrar los datos que circulan por internet en múltiples capas, como una cebolla (de ahí su nombre, The Onion Router), y los envía a través de diferentes servidores administrados por voluntarios, hasta que llegan a su destino. Al rebotar tanto la información, hace que tu actividad sea extremadamente difícil de rastrear.

La red TOR se ha convertido en una herramienta crucial para denunciantes, disidentes, periodistas, activistas y personas que buscan esquivar sistemas de vigilancia en la red. También es útil para acceder a sitios web bloqueados por gobiernos o proveedores de servicios de internet y a información solo accesible en la internet oculta (web profunda y web oscura). Esos espacios ocultos utilizan en sus URL el dominio .onion, en lugar de los comunes de la web visible (.com, .org, .net, .edu, .gob, .es, etc.).

**Figura 3. Campaña de los desarrolladores de la red TOR lanzada en octubre de 2020, en el contexto de la pandemia de covid-19**


Fuente: https://www.torproject.org/

Algunos de los medios periodísticos más prestigiosos del mundo tienen dominios «cebolla» para navegar por sus sitios de manera segura, anónima y sin censura. Algunos ejemplos (tienes que usar TOR):

- **The Guardian**
  https://www.guardian2zotagl6tmjucg3lrhxdk4dw3lhbqnkvvkywawy3oqfoprid.onion
- **BBC News**
  https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion
- **ProPublica**
  http://p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion
- **The Intercept**
  https://gm64cjz7un7ucso4yegkssuqfzmg7ctn7mkb66c7l6sj7gzyo6syphid.onion

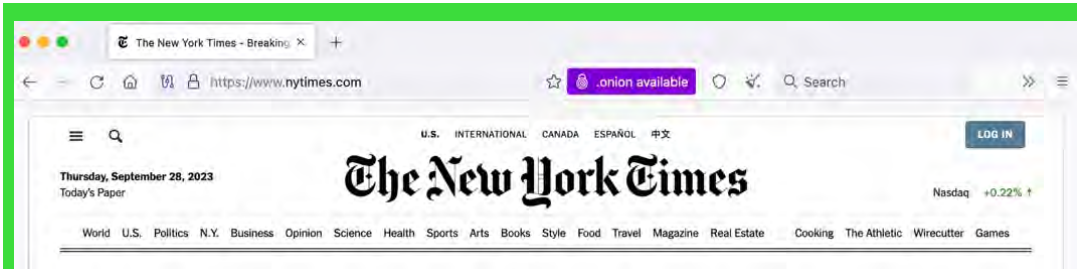
- **The New York Times**
  https://www.nytimesn7cgmftshazwhfgzm37qx-b44r64ytbb2dj3x62d2lljsciiyd.onion
- **Deutsche Welle**
  https://dwnewsgngmhlplxy6o2twtfgjnrnjxbegbwqx6w-notdhkzt562tszfid.onion/en/top-stories/s-9097
- **RadioFreeEurope**
  https://www.rferlo2zxgv23tct66v45s5mecftol-5vod3hf4rqbipfp46fqu2q56ad.onion
- **Bellingcat**
  http://bellcatmbguthn3age23lrbseln2lryz-v3mt7whis7ktjw4qrestbzad.onion

También puedes acceder a algunas redes sociales convencionales por TOR para evitar que te rastreen. Por ejemplo:

- **Facebook**
  https://www.facebookwkhpilnemxj7asaniu7vn-jjbiltxjqhye3mhbshg7kx5tfyd.onion
- **Twitter**
  https://twitter3e4tixl4xyajtrzo62zg5vztm-juricljdp2c5kshju4avyoid.onion
- **Reddit**
  https://www.reddittorjg6rue252oqsxryoxen-gawnmo46qy4kyii5wtqnwfj4ooad.onion

Una forma de saber si un sitio de la web visible es accesible en la oscura es cargando en TOR su URL convencional (por ejemplo, https://www.nytimes.com/ o https://www.twitter.com/) y observar si en la barra de direcciones hay un botón de acceso «onion disponible».

**Figura 4. URL convencional de The New York Times cargada en el navegador TOR, con botón de acceso a su versión «cebolla»**




Fuente: The New York Times

TOR tiene un motor de búsqueda predefinido. Se trata de DuckDuckGo (https://duckduckgo.com/), que no registra ni almacena tus consultas para proteger tu privacidad. Su lema es «Busca en la Red sin que te rastreen». Por supuesto, la web oscura no está libre de informaciones falsas, contenidos ilícitos o ilegales y espacios peligrosos y perturbadores. Si usas TOR para introducirte en ella, debes hacerlo con extrema responsabilidad y precaución.

## 3.2. Si no te gusta la cebolla…

Si buscas un navegador más «amigable» y rápido que TOR, más parecido a los navegadores convencionales, una alternativa es Brave (https://brave.com/). Sus desarrolladores presumen de que es «más rápido que Chrome» y «más seguro que Safari». Algunas de sus características más destacadas son que bloquea publicidad, huellas digitales, cookies y rastreadores de anuncios de forma predeterminada.

Además, puedes importar a Brave marcadores, extensiones y contraseñas de otros navegadores. También ofrece un servicio personalizado y privado de tus fuentes de información (redes sociales, blogs, prensa…) en un único canal que se actualiza au-

tomáticamente. Sus creadores afirman que «Noticias de Brave no rastrea lo que sigues, lees o clicas».

Aunque puedes utilizar cualquier buscador, Brave tiene uno propio: https://search.brave.com/. Su lema: «Haz búsquedas sin dejar rastro». En su sitio web, sus desarrolladores presumen de que «Brave no controla tus búsquedas», ya que «son confidenciales», lo que lo convierte en una «alternativa real a Google».

A diferencia del proyecto TOR (sin ánimo de lucro), Brave sí tiene un modelo de negocio, pero se diferencia notablemente del de Google: se basa en anuncios no intrusivos y respetuosos con la privacidad, sin rastreadores ni cookies, y por los que se paga tanto a anunciantes como a usuarios cuando estos últimos ven la publicidad (los usuarios deciden si quieren ver o no publicidad y qué tipos de anuncios quieren que se les muestre).

Si quieres echarle «cebolla» a Brave, puedes usar su «modo TOR» para conectarte a esta red por una ventana privada que no almacena tu navegación, pero como recomiendan los creadores de Brave, «si tu seguridad depende de permanecer en el anonimato, utiliza TOR en su lugar».

Otra opción de seguridad de Brave es una VPN (red privada virtual) integrada para cifrar y proteger todo lo que haces. Pero en este caso es un servicio de pago.

Firefox es otra alternativa para el usuario medio. Desarrollado por la Fundación Mozilla (https://www.mozilla.org/), es, como TOR, un software libre y de código abierto. Entre sus características destaca la «protección antirrastreo mejorada» para bloquear muchos de los rastreadores que recopilan información sobre tus hábitos de navegación e intereses.

Mozilla (organización sin ánimo de lucro) ofrece también una VPN para cifrar tu actividad y ocultar tu IP. Como la de Brave, también es de pago.

Firefox incorpora un servicio gratuito para guardar contenidos en una biblioteca personal: Pocket (https://getpocket.com/). Y también puedes usar distintos motores de búsqueda, aunque una de las críticas más feroces a Mozilla ha sido su decisión de hacer de Google el buscador predeterminado de Firefox, algo que parece contradecir los principios éticos de esta fundación.

Por último, y como curiosidad, TOR está basado en Firefox.

## →04.
## Sáltate el protocolo

En 1991, el científico computacional Tim Berners-Lee abrió a todo el mundo, tras dos años de trabajo, la «world wide web» (comúnmente conocida como www, w3, o la web), el sistema que popularizó el acceso a internet. El protocolo de transferencia de hipertexto, el «http» (hypertext transfer protocol), sobre el que se basa la «www», se convirtió en el estándar que todos usamos para acceder a la red.

La «www» fue un regalo de Berners-Lee a la humanidad. Decidió no patentarla y su código fuente fue liberado. Pero gigantes tecnológicos y gobiernos se hicieron con su control, contra la voluntad de Berners-Lee, cuya aspiración sigue siendo una web libre y descentralizada, ahora con el proyecto Solid:

https://solidproject.org/

Pero para conectarse a internet existen otros protocolos, variados por sus características y funciones: Telnet, FTP, SSH, IRC, BitTorrent, GNUnet... Aquí explicaré uno para navegar por una internet alternativa a la de la masificada y controlada «www». Debemos remontarnos de nuevo a 1991.

Mientras Berners-Lee ultimaba la «www», un equipo de la Universidad de Minnesota (Estados Unidos) liderado por el científico computacional Mark P. McCahill presentó el proto-

colo Gopher, el cual fue descrito como una forma sencilla de navegar por recursos de información distribuidos en internet, pero sin hipervínculos. Esta fue una desventaja respecto a la «www» y su http, pero hasta que esta no empezó a popularizarse, Gopher fue el protocolo de referencia.

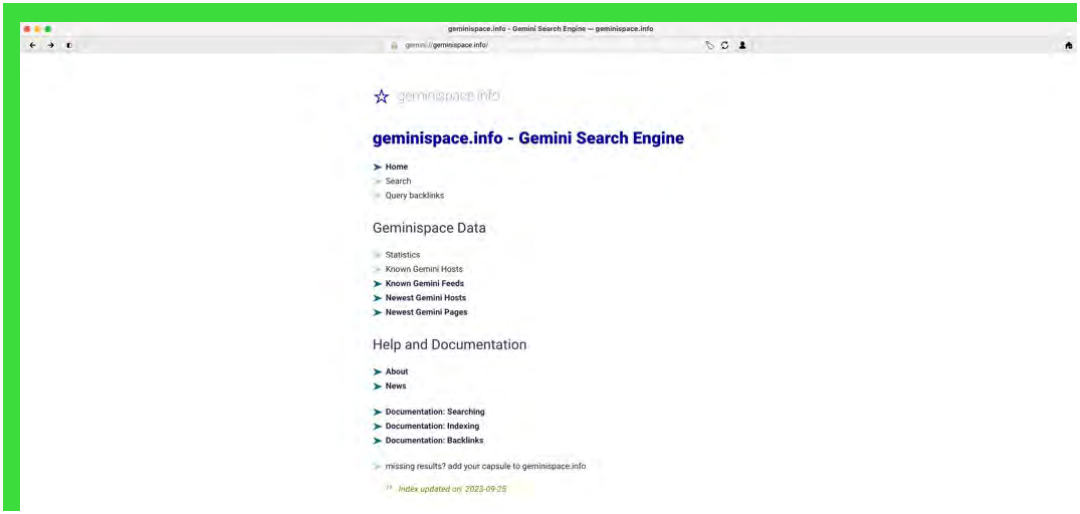
En 1992, seis años antes de que Google estrenase su buscador, Gopher presentó el primer gran motor de búsquedas en internet para archivos de texto sin formato, Veronica (Very Easy Rodent-Oriented Net-wide Index to Computer Archives).

La popularidad de Gopher se desplomó a finales del siglo XX. La w3 se convirtió en el sistema preferido para acceder a internet gracias al hipertexto, su capacidad multimedia, el desarrollo de navegadores amigables y de buscadores como Google o Yahoo!, y la oportunidad de negocio que abrió a empresas de todo el mundo.

Ahora, otro protocolo está recuperando las esencias de Gopher. Su nombre, Gemini (https://geminiprotocol.net/). Sus desarrolladores describen así este proyecto de código abierto iniciado en 2019:

> *«Gemini no se trata de innovación o disrupción, se trata de brindar un respiro a aquellos que sienten que internet ya ha sido suficientemente perturbada. No pretendemos cambiar el mundo ni destruir otras tecnologías. Nuestro objetivo es construir un espacio en línea liviano donde los documentos sean solo documentos, en interés de la privacidad, la atención y el ancho de banda de cada lector» (Project Gemini, s.f.).*

**Figura 5. Vista del buscador geminispace.info con el navegador Lagrang**




Fuente: https://geminispace.info

Gemini facilita una experiencia más liviana, rápida y segura, basada más en texto que en contenidos multimedia, sin publicidad ni cookies ni mecanismos de rastreo. Se dice que Gemini es una web simplificada y un Gopher modernizado.

Lo que llamamos sitios web en la w3 se denominan cápsulas en Gemini. Sus URL no comienzan por http:// ni https://, sino por gemini://. A 16 de septiembre de 2023, Gemini contabilizaba 640.902 páginas y 2.237 dominios, según datos de geminispace.info/statistics

Gemini protege tu privacidad con el protocolo criptográfico TLS (Transport Layer Security) y cada solicitud de conexión es independiente de las demás, por lo que no hay forma de rastrearte al navegar entre cápsulas.

Gemini es interesante para personas que valoran su privacidad, rechazan el sistema de seguimiento en la web y están hartas de molestas ventanas emergentes, anuncios intrusivos

o vídeos que se reproducen automáticamente. También lo es para internautas con una conexión lenta o consumo de datos limitados, y para quienes gozan de lecturas pausadas y sin distracciones. Gemini es también una buena alternativa para quien quiera «desinfoxicarse», es decir, liberarse del exceso de información (infoxicación) que recibimos por la web y que satura nuestra capacidad para discernir si las fuentes son confiables o no y si la información recibida es verídica o falsa.

Para generar contenido en Geminispace existen varias opciones. Una buena manera de empezar para un novato es mediante servicios de alojamiento multiusuario en la web. Entre estos destaca Gemlog Blue (https://gemlog.blue/), donde el contenido termina publicado exclusivamente en Geminispace. Pero también puedes publicar simultáneamente para Gemini, la web y Gopher con Flounder (https://flounder.online/) o Smol Pub (https://smol.pub/). Y si te atreves con servicios nativos de Gemini, puedes probar Bubble (gemini://skyjake.fi/bubble/) o Station (gemini://station.martinrue.com/).

Hay otras vías para publicar, aunque la que te ofrece mayor independencia, libertad y control es configurar tu propio servidor Gemini en un VPS (servidor privado virtual) o en una computadora. El Proyecto Gemini ofrece una lista de software de servidor: https://geminiprotocol.net/software/.

¿Y para navegar por Geminispace? Existen distintas vías con diferentes grados de complejidad. Tanto para ordenadores personales como para móviles hay varios navegadores, entre los que se puede destacar Lagrange (https://gmi.skyjake.fi/lagrange/), que tiene versiones para Windows, macOS y Linux (escritorio) e iOS y Android (móvil). En estos enlaces encontrarás más alternativas:

- https://geminiprotocol.net/clients.html
- https://github.com/kr1sp1n/awesome-gemini

# 05. Usenet, regreso a los orígenes de las redes sociales

Otra señal de que la «vieja internet» (también conocida como la «Internet independiente», «pequeña internet» e «internet alternativa») está regresando es el resurgir de Usenet (Users Network), la primera red social en línea, anterior a la world wide web.

Usenet fue creado en 1979 por Tom Truscott y Jim Ellis en la Universidad de Duke (Estados Unidos). En la década de 1980 ganó fama entre los pocos y aventajados internautas que había entonces. En la década de 1990 aún era un sistema popular de comunicación entre redes de computadoras, pero con el desarrollo de la w3, de las redes sociales comerciales, de los contenidos multimedia, de servicios de correo como Gmail o Outlook y de aplicaciones de mensajería instantánea, su uso fue en declive... hasta que ha resurgido.

Básicamente, es una red federada y descentralizada de igual a igual (peer-to-peer) que alberga «grupos de noticias» distribuidos en servidores, algunos moderados, otros no. Los usuarios de cada servidor se agrupan en temáticas (listas de grupos) para compartir información y debatir. Y se organizan con una estructura jerárquica, de manera que hay grupos principales (jerarquías) con muchos subgrupos a varios niveles. Las principales jerarquías son:

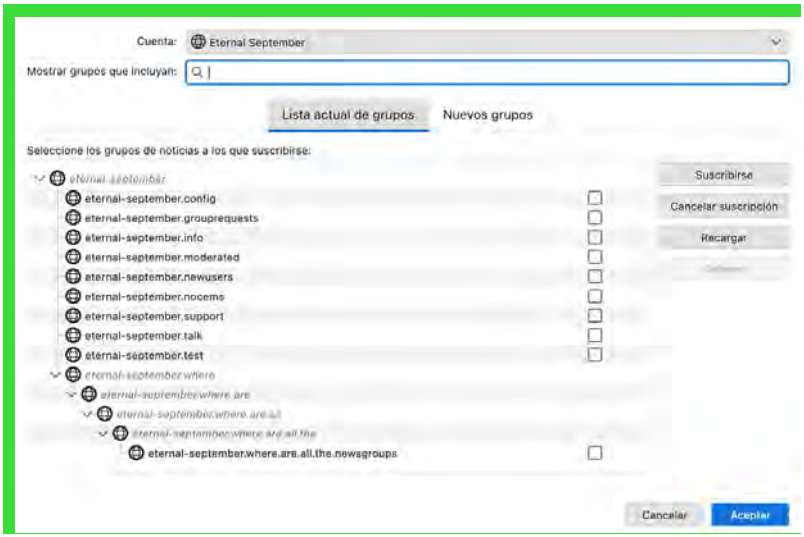
- *comp.** Computación
- *humanities.** Humanidades
- *misc.** Miscelánea de temas
- *news.** Temas sobre Usenet
- *rec.** Actividades recreativas
- *sci.** Ciencia

- *soc.** Temas sociales
- *talk.** Discusiones de temas controvertidos
- *alt.** Temas alternativos y populares

También existen jerarquías de países, idiomas, regiones o áreas locales, como *de.** (Alemania), *uk.** (Reino Unido), *es.** (España), *esp.** (idioma español), *ca.** (California), *chi.** (Chicago), etc. Y muchas más sobre temas tan diversos como *yale.** (Universidad de Yale), *microsoft.** (productos de Microsoft), *gnu.** (el sistema operativo de software libre GNU), *gov.** (temas gubernamentales), *bionet.** (biología), *biz.** (negocios), etc.

El protocolo de Usenet para la transferencia de noticias en red es NNTP (Network News Transfer Protocol). Para proteger a los usuarios se suele aplicar la tecnología de encriptación SSL/TLS (Secure Socket Layer/Transport Layer Security), con la que nadie –ni siquiera tu ISP– puede ver a qué grupos y publicaciones accedes.

**Figura 6. Suscripción mediante Thunderbird a grupos de noticias del servidor news.eternal-september.org**




Fuente: news.eternal-september.org

Usenet se ha erigido en uno de los paradigmas de la libertad de expresión y de información de la internet descentralizada. Por su naturaleza, es una red resistente a la censura (otra forma de desinformación). Pero, como todo espacio virtual o físico, está también expuesto a información falsa y dañina, aunque se confía en la capacidad de sus comunidades para frenarla.

Para conectarte debes obtener una cuenta en un servidor Usenet, instalar un cliente (lector de noticias o newsreader), indicarle la dirección del servidor, descargar su lista de grupos y suscribirte a los que quieras.

Existen diferentes clientes. Para un usuario no experto, uno popular y sencillo es Thunderbird (https://www.thunderbird.net/), un producto de Mozilla de código abierto y gratuito para macOS, Windows y Linux. Para configurar Thunderbird y conectarte consulta estos enlaces:

- http://mzl.la/1ApHin9
- https://www.big-8.org/wiki/Getting_Started_with_Usenet

## 06. Viaja al Fediverso

La última propuesta es un viaje por un mundo alternativo al de las plataformas sociales de las «big tech» donde el poder y la soberanía de los datos y algorítmica residen en los usuarios: el Fediverso.

### 6.1. Federados, libres y seguros

Desde que el magnate Elon Musk compró Twitter (renombrada X) el 27 de octubre de 2022, otra plataforma social aparentemente similar en su interfaz, pero totalmente opuesta en su

filosofía, Mastodon, empezó a ganar popularidad. Y con ella, el Fediverso, del que es parte.

Fediverso es el acrónimo de «federación» y «universo». Es un conjunto de servidores interconectados para publicaciones en la web (microblogging, blogs, vídeos, fotos...). Aunque los servidores (conocidos como instancias) son independientes, pueden comunicarse entre sí, facilitando la interoperabilidad, de manera que usuarios de una instancia pueden interactuar con los de otra y con otras plataformas. Esto no ocurre en las redes comerciales, donde es imposible interactuar, por ejemplo, entre usuarios de Twitter, Instagram y TikTok. El principal protocolo para la interoperabilidad del Fediverso es ActivityPub (https://activitypub.rocks/), recomendado por el World Wide Web Consortium:

https://www.w3.org/TR/activitypub/

El Fediverso es, en definitiva, un conjunto de tecnologías y protocolos abiertos que permiten interconectar un cúmulo de redes sociales descentralizadas, libres, autónomas y federadas, sin ánimo de lucro, sin publicidad integrada y centradas en proteger la privacidad de sus usuarios, sin una autoridad central que dicte reglas, sin algoritmos que nos condicionen o favorezcan a unos usuarios o publicaciones sobre otros, sin una empresa que recolecte nuestros datos y trafique con ellos. Además, todo el Fediverso se ejecuta con software libre y de código abierto.

Cualquiera puede ejecutar y administrar su propio servidor y federarlo a otras instancias (comunidades). O, como usuario, puedes buscar entre la variada lista de proyectos del Fediverso (distintas plataformas y softwares) e instancias y elegir dónde registrarte en función de la actividad que quieras realizar y de tus intereses.

A 23 de septiembre de 2023, The Federation (https://the-federation.info/) –sitio de referencia para estadísticas del Fediver-

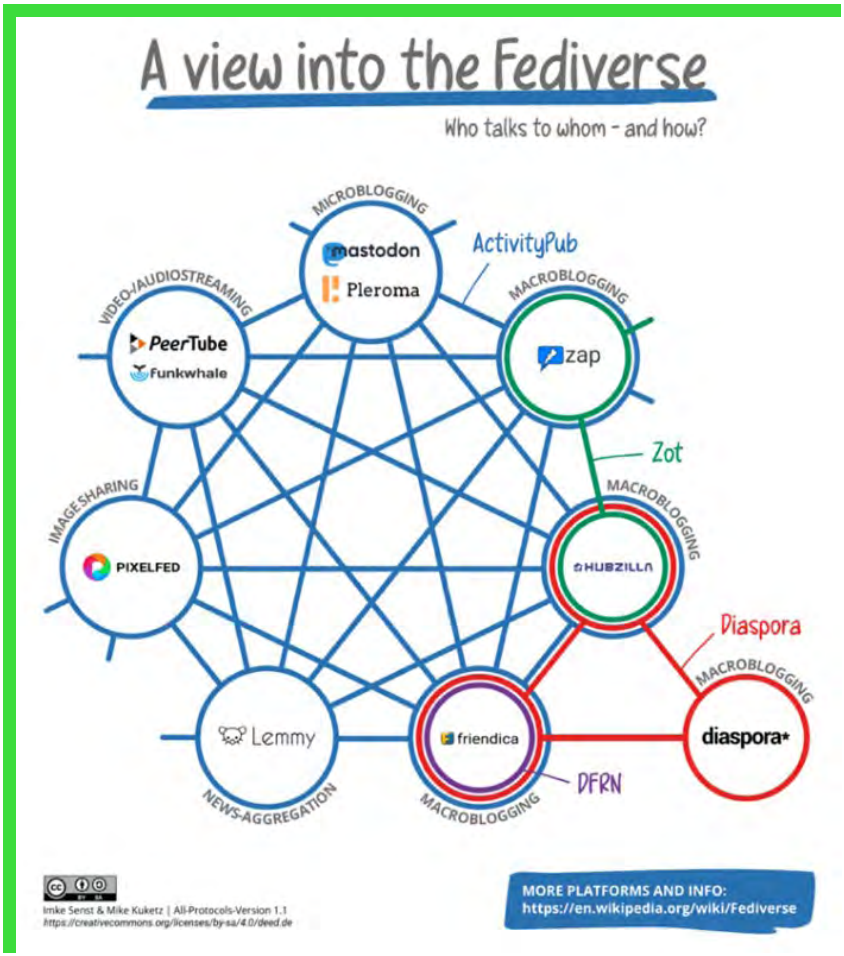
so– recogía 148 proyectos sobre 16 protocolos, 26.813 nodos y 13.552.977 usuarios.

- **Proyectos:** son los softwares libres y de código abierto sobre los que se construyen las plataformas del Fediverso (Mastodon, Pleroma, PeerTube, Pixelfeld, Friendica, GNU Social, Lemmy, Funkwhale, Mobilizon, Diaspora, Misskey, Hubzilla, Matrix, etc.) y cada uno de ellos está diseñado para un fin (fotos, vídeos o audio, blogs o microblogs, foros de discusión, organización de eventos...); son los equivalentes del Fediverso a redes comerciales como Twitter, Facebook, Instagram, YouTube, TikTok, etc.
- **Protocolos:** existen distintos protocolos de red abiertos y descentralizados para la comunicación entre instancias y plataformas (interoperabilidad), aunque el más popular es ActivityPub; así, un usuario de una instancia de Mastodon puede interactuar con los de otras instancias de este proyecto, pero también puede hacerlo con otras plataformas con el mismo protocolo.
- **Nodos:** son las instancias (servidores) de cada proyecto; cada instancia es una red social autónoma en cada plataforma, con administradores y usuarios que pueden federarse con otras instancias.

## 6.2. Alternativas a las redes comerciales

Para cada plataforma de las «big tech» existen alternativas en el Fediverso. Aquí te propongo algunas de las más populares entre la larga lista de proyectos federados. Todas usan ActivityPub y son interoperables.

**Figura 7. Esquema del Fediverso**




Fuente: File: Fediverse AllProcotols v1.1 13.05.2022.png. (2022, 3 de julio). Wikimedia Commons (CC BY-SA 4.0).

## TWITTER - MASTODON

Mastodon es el proyecto más popular del Fediverso. Ganó fama cuando Elon Musk compró Twitter y cambió algunas normas y usos para esta plataforma que generaron gran polémica y descontento entre muchos usuarios que buscaron refugio en Mastodon por su aparente similitud. Pero Mastodon ya existía

desde octubre de 2016. Su lema: «Una red social que no está a la venta». Hay una gran variedad de instancias con sus normas y guías para cada comunidad, o como en cualquier otra plataforma federada, puedes crear la tuya propia. Las publicaciones se presentan en orden cronológico, de manera que no hay usuarios y contenidos destacados por algoritmos o por pagos publicitarios o promocionales. Más información:

https://joinmastodon.org/es

### ❷ INSTAGRAM -PIXELFELD

Esta plataforma de fotos y vídeos es muy similar a Instagram en su interfaz y usabilidad, pero se diferencia de la red de Meta en que no tiene publicidad, tus datos no se envían ni se venden a terceros y no hay algoritmos que limiten quién ve tus publicaciones, ya que todas se presentan en orden cronológico. Más información:

https://pixelfed.org/

### ❸ YOUTUBE - PEERTUBE

PeerTube es la principal alternativa federada a YouTube. Te permite crear tu plataforma de vídeo independiente. Sus desarrolladores presumen de que es un proyecto libre de «algoritmos opacos» y de «políticas de moderación incomprensibles» como en YouTube. PeerTube tampoco depende de publicidad y no rastrea tus datos. Más información:

https://joinpeertube.org/

### ❹ TWITCH - OWNCAST

Twitch se ha posicionado como el gran rival de YouTube en el ecosistema de plataformas de vídeo de las «big tech». Está diseñado para la retransmisión en directo. En el Fediverso, Owncast es la principal alternativa a Twitch. Sus desarrolladores destacan que «puede llegar a una audiencia más amplia en el

Fediverso, permitiendo a las personas seguirla y compartirla en Mastodon y otros servicios federados». Más información:

https://owncast.online/

### ❺ SPOTIFY - FUNKWHALE

Spotify es la plataforma comercial que domina la música en streaming. Funkwhale es la principal alternativa del Fediverso a Spotify y servicios similares. Este proyecto promueve la publicación de archivos sonoros con licencias creative commons, las cuales permiten que sean copiados, distribuidos, editados, remezclados y usados por otros, pero reconociendo la autoría original y bajo determinadas condiciones. Más información:

https://funkwhale.audio/

### ❻ PLATAFORMAS DE PODCASTS - CASTOPOD

Para los amantes de los podcasts que buscan plataformas alternativas, una opción del Fediverso especializada en este formato es CastoPod. Su filosofía se resume en esta frase: «Tu podcast y tu audiencia te pertenecen a ti y solo a ti». Este software no solo facilita la interoperabilidad con otras plataformas federadas, también permite que tus podcasts aparezcan en plataformas comerciales como Apple Podcasts, Spotify, Deezer, Podcast Addict, Podfriend..., o exportarlos a redes como Twitter, Instagram, Youtube o Facebook. Además, puedes monetizar tus contenidos con suscripciones premium, micropagos, propinas o anuncios de audio sin cookies. Más información:

https://castopod.org/

### ❼ GRUPOS Y EVENTOS EN FACEBOOK - MOBILIZON

«Reunir, organizar, movilizar». Sobre estas ideas se desarrolla Mobilizon, la alternativa del Fediverso a los eventos y grupos de Facebook. Aquí puedes buscar o anunciar actividades,

o crear una página para organizar grupos. Como explican sus desarrolladores, «Mobilizon no es una plataforma social ni una herramienta de comunicación viral; sería más adecuado considerarlo un espacio autónomo para tu grupo, donde los miembros podrán seguir nuevos contenidos». Más información:

https://joinmobilizon.org/es/

### 8 GOODREADS - BOOKWYRM

Las comunidades de lectores abundan en la web. Sus usuarios catalogan, valoran y recomiendan libros, contribuyendo al éxito o al fracaso de autores y sus obras, junto con el poder de los algoritmos. La más conocida es Goodreads, de Amazon. Una opción del Ferdiverso es BookWyrm, para llevar un registro de tus lecturas, hablar sobre libros, escribir reseñas y descubrir nuevas lecturas. Aquí, como en todo el Fediverso, la popularidad se gana sin trucos algorítmicos. Más información:

https://joinbookwyrm.com/es/

### 9 MEDIUM - WRITEFREELY

Para los amantes de los blogs minimalistas, la versión de Medium en el Fediverso es WriteFreely. Como se destaca en su sitio, ofrece tanto a escritores como a lectores un entorno limpio y libre de distracciones, «sin notificaciones», «me gusta» o «aplausos innecesarios». Los usuarios de cualquier plataforma federada con el mismo protocolo pueden seguir tu blog, marcar tus publicaciones como favoritas y compartirlas. Más información:

https://writefreely.org/

### 10 REDDIT - LEMMY

Lemmy es la plataforma federada más conocida para la agregación de enlaces sociales y foros de discusión, similar a Reddit. El contenido se organiza en comunidades, de manera que

te puedes suscribir a las que más te interesen. Cada instancia puede establecer su política de moderación para evitar spam y trolls, y los votos de la comunidad a favor o en contra influyen en el contenido que aparece destacado. Aquí tampoco hay publicidad, rastreadores ni algoritmos opacos. Más información:

https://join-lemmy.org/

### 11 WHATSAPP - MATRIX

Entre las tecnologías de mensajería instantánea, Matrix es la alternativa del Fediverso a WhatsApp y aplicaciones similares, como Telegram, Discord, Teams, Slack o iMessage. En realidad, Matrix no es una aplicación, sino un protocolo de código abierto que ofrece interoperabilidad y comunicaciones descentralizadas y seguras con cifrado de extremo a extremo. Es desarrollado por la organización sin ánimo de lucro Matrix.org Foundation. Sus orígenes se remontan a 2014, aunque empezó a ganar millones de usuarios en la década de 2020. Puedes enviar en tiempo real mensajes, compartir archivos o hacer llamadas de voz y vídeo. Cualquiera puede crear un cliente de Matrix, alojar su servidor y comunicarse con otros usuarios, independientemente del servidor que usen. Además, puedes crear «puentes» para conectar Matrix a WhatsApp, Telegram, Discord, Slack, Signal, Messenger, Google Chat, Instagram, LinkedIn, Twitter, Skype o iMessage, entre otros. Aunque hay diversas maneras de usar Matrix, la más fácil para iniciarse es mediante el cliente Element, una aplicación multiplataforma de Matrix.org Foundation.

Más información:

https://matrix.org/

https://joinmatrix.org/

https://element.io/

La lista de proyectos del Fediverso es amplia. Aquí puedes encontrar más:

- https://the-federation.info/#projects
- https://fediverse.info/explore/projects
- https://fediverse.party/en/miscellaneous/

# bibliografía


Bradshaw, S. (2019). *Disinformation optimised: gaming search engine algorithms to amplify junk news.* Internet policy review, 8(4). https://doi.org/10.14763/2019.4.1442

d'Ancona, M. (2019). *Posverdad: La nueva guerra en torno a la verdad y cómo combatirla.* Madrid: Alianza Editorial.

Dhawan, S., Hegelich, S., Sindermann, C. y Montag, C. (2022). *Re-start social media, but how?* Telematics and Informatics Reports, 8, 100017. https://doi.org/10.1016/j.teler.2022.100017

Ferraris, M. (2019). *Posverdad y otros enigmas.* Madrid: Alianza Editorial.

Hoffmann, S., Taylor, E. y Bradshaw, S. (2019, 11 de octubre). *The market of disinformation.* Oxford Information Labs. https://oxtec.oii.ox.ac.uk/publication/the-market-of-disinformation/

Kaiser, B. (2019). *La dictadura de los datos: La verdadera historia desde dentro de Cambridge Analytica y de cómo el Big Data, Trump y Facebook rompieron la democracia y cómo puede volver a pasar.* Madrid: HarperCollins Ibérica.

Li, H.O.Y., Bailey, A., Huynh, D. y Chan, J. (2020). *YouTube as a source of information on COVID-19: a pandemic of misinformation?* BMJ global health, 5(5), e002604. http://dx.doi.org/10.1136/bmjgh-2020-002604

McIntyre, L. (2018). *Posverdad.* Madrid: Ediciones Cátedra.

Míguez González, M.I., García Crespo, O. y Ramahí García, D. (2020). *Análisis de vídeos sobre cáncer de mama en YouTube.* Cuadernos.Info, (44), 179–193. https://doi.org/10.7764/cdi.44.1528

Quian, A. (2022). *Civilización hacker.* Madrid: Anaya Multimedia.

Reviglio, U. y Agosti, C. (2020). *Thinking outside the black-box: the case for «algorithmic sovereignty» in social media.* Social Media + Society, 6(2) https://doi.org/10.1177/2056305120915613

Shah, C. (2021, 10 de marzo). *It's not just a social media problem–how search engines spread misinformation.* The Conversation. https://theconversation.com/its-not-just-a-social-media-problem-how-search-engines-spread-misinformation-152155

Snowden, E. (2019). *Vigilancia permanente.* Barcelona: Planeta.

Véliz, C. (2021). *Privacidad es poder: datos, vigilancia y libertad en la era digital.* Barcelona: Debate.

Vosoughi, S., Roy, D. y Aral, S. (2018). *The spread of true and false news online.* Science, 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Zuboff, S. (2020). *La era del capitalismo de la vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder.* Barcelona: Ediciones Paidós.