

La ventaja de la atención: cómo las empresas de Internet se aprovechan del consumidor desinformado

The attention advantage: how Internet companies profit from the uninformed consumer

A vantagem da atenção: como as empresas da Internet se aproveitam do consumidor desinformado

Olivia Llanio

B.A. Internet, Cultures and Social Evolutions and Political Science (Rollins College, USA)
<https://orcid.org/0009-0009-0751-6409>
ollanio@rollins.edu

Resumen

Este artículo presenta un análisis del papel del/a consumidor/a en una internet social. Repasa las prácticas de privacidad y recopilación de datos, las empresas modernas de medios de comunicación, la publicidad digital, y las repercusiones a las que se enfrentan los/as consumidores/as y usuarios/as en el actual panorama digital. Explica el panorama de la intermediación de datos y el papel que desempeñan las empresas tecnológicas modernas en la economía digital. Este análisis establece conexiones entre lo informados que están los/as consumidores/as y cómo se comportan en línea, argumentando que las empresas que poseen diversos medios se benefician de los/as consumidores/as desinformados/as. El documento proporciona el contexto crítico de las grandes empresas de internet con ánimo de lucro, dentro de un ecosistema en el que opera la mayoría de la población mundial. Esta comprensión sienta las bases de la investigación relacionada con las economías digitales y la participación en los medios de comunicación en línea, y puede brindar a los/as usuarios/as la oportunidad de tomar decisiones más informadas a nivel individual y político.

Palabras clave: Empresas de medios de comunicación, medios sociales, privacidad digital, intermediación de datos, atención, datos, Internet.

Abstract

This paper presents an analysis of the role of a consumer in a social internet. It reviews privacy and data collection practices, modern media companies, digital advertising, and the impacts consumers and users

face in the current digital landscape. It explains the landscape of data brokerage and the role modern technology companies have in the digital economy. This analysis draws connections between how informed consumers are and how they behave online, arguing that mixed media companies benefit from uninformed consumers. The paper provides the critical context of large, for-profit internet companies within an ecosystem that the majority of the global population operates within. This understanding sets the foundation for research related to digital economies and media engagement online and can equip users with an opportunity for more informed decision making at the individual and policy levels.

Keywords: Media companies, social media, digital privacy, data brokerage, attention, data, internet.

Resumo

Este artigo apresenta uma análise do papel do consumidor numa Internet social. Passa em revista as práticas de privacidade e de recolha de dados, as empresas modernas de comunicação social, a publicidade digital e as implicações que os consumidores e os utilizadores enfrentam no atual panorama digital. Explica o panorama da intermediação de dados e o papel das empresas tecnológicas modernas na economia digital. Esta análise estabelece ligações entre o grau de informação dos consumidores e o seu comportamento em linha, argumentando que as empresas proprietárias de meios de comunicação social beneficiam de consumidores desinformados. O documento fornece um contexto crítico para as grandes empresas de Internet com fins lucrativos num ecossistema em que opera a maioria da população mundial. Esta compreensão lança as bases para a investigação relacionada com as economias digitais e a participação nos meios de comunicação social em linha, e pode dar aos utilizadores a oportunidade de tomarem decisões individuais e políticas mais informadas.

Palavras-chave: Empresas de comunicação social, redes sociais, privacidade digital, intermediação de dados, atenção, dados, Internet.

Introducción

Internet ha evolucionado drásticamente en unas pocas décadas. Algo que fue casi irrelevante se ha convertido en convencional, pasando del acceso abierto a un paisaje de comercialización y sitios de pago. A lo largo de este tiempo, muchas grandes empresas de este sector han surgido y desaparecido, y pocas han seguido siendo líderes en sus sectores. Hoy en día, la frontera digital está prácticamente monopolizada. Las pocas empresas que lideran el sector se conocen como las «Cinco Grandes». Las «Cinco Grandes» se refieren a Alphabet (la empresa matriz de Google), Amazon, Meta (antes Facebook), Apple y Microsoft. Son los magnates de su tiempo, acumulando niveles récord de riqueza, poder y control

de la industria. Estas empresas tienen numerosos enfoques para ganar sus miles de millones, varios en común. Juntas, establecen las normas del sector, y las imponen mediante su control del mercado.

El grado de control que ejercen sobre sus industrias hace de ello una cuestión fundamental de investigación. Este artículo se centra en las facetas no relacionadas con el hardware, sino orientadas a los datos de las operaciones de estas empresas. En concreto, las áreas comerciales de las redes sociales, las búsquedas en línea y los servicios en la nube. Estos sectores generan enormes beneficios, a la vez que proporcionan acceso gratuito. Sus métodos habituales de obtención de beneficios no son muy conocidos por su transparencia y, por lo general, están al menos parcialmente ocultos para la persona usuaria media. Este documento explicará el contexto social, sus economías, y cómo las principales empresas del mercado de servicios digitales se benefician de que sus consumidores/as estén desinformados/as sobre la realidad del funcionamiento de estos servicios gratuitos.

El panorama digital moderno

Estar en línea hoy en día es estar rodeado de ruido. La empresa digital de éxito mantiene la atención del usuario el mayor tiempo posible, a través de contenidos cada vez más atractivos, y del diseño de su plataforma. Con la realidad de ese panorama, es fácil comprender el desbordamiento de información. Esto, unido a los específicos sitios informativos que consulta la mayoría, está delicadamente diseñado para que se disfrute sin muchas preguntas. Así lo impulsan y ejemplifican los magnates de las redes sociales e internet de hoy en día. Centrarnos en los servicios que ofrecen la jerarquía capitalista de las «Cinco Grandes» permitirá establecer paralelismos específicos entre empresas y plataformas.

Este artículo se centra en Meta (Facebook, Instagram), Google y Twitter. Tanto Meta como Google -dos gigantes en sus respectivos ámbitos tecnológicos- se incluyen aquí porque, aunque su cartera de software difiere entre sí, tienen flujos de ingresos que, para el ámbito de este documento, son razonablemente similares. La atención se centra en empresas cuya función principal está en el espacio de las redes sociales, donde la investigación pertinente se aplica a sus ramas de medios de comunicación y/o publicidad. Twitter y Meta son líderes en el espacio de redes sociales, con sus vastas bases de usuarios y su capital social. La plataforma más conocida de Google es YouTube, pionera en el espacio de marketing de medios sociales en 2010. Google también alberga anuncios en sus servicios digitales, como Gmail y Google Maps.

Todas estas empresas producen contenidos multimedia variados: visual, auditivo y escrito. Incluye películas, programas, podcasts y música, artículos de noticias, e imágenes y vídeos breves. En la actualidad, cualquiera de estos tipos de contenido puede encontrarse en las redes sociales. Por lo general, esto genera y mantiene la actividad de las personas en las plataformas. Más tradicionalmente, la clientela solía pagar por el acceso a los propios medios. Los periódicos, los CDs, y la televisión por cable, son ejemplos de esa práctica. Los ingresos generados por los propios medios constituyen un modelo mercantil conocido como «modelo de contenido de los medios» (Fuchs, 2020). Fuchs considera que el modelo de contenido mediático es uno de los diversos «modelos de acumulación de capital» (2020, p. 152) y forma parte integral de las estrategias de venta de las empresas de medios sociales modernos.

Las empresas que generan ingresos mediante la publicidad en sus plataformas no son nuevas. Tampoco lo es el solapamiento entre estos modelos de contenido y publicidad. La fusión de estos modelos de venta se describe mejor mediante lo que Fuchs denomina «empresas de medios mixtos» (2020). Las empresas de medios mixtos venden, o mercantilizan, con más de un enfoque de ventas:

Las empresas de medios mixtos tienen al menos una forma dual de la mercancía: La atención de la audiencia (C'2) se vende a los clientes publicitarios. Al menos otra mercancía (C'1) se vende a los clientes. C'1 suele ser el contenido, pero también puede ser otra mercancía comunicativa, como las tecnologías de la comunicación. (Fuchs, 2020, p. 145).

Las empresas de medios mixtos (MMC) combinan diferentes modelos de negocio para generar múltiples fuentes de ingresos al mismo tiempo, son más matizadas y complejas que cualquiera de los modelos mencionados por sí solos, debido a sus servicios compuestos. Las MMC no siempre se componen de modelos estrictamente mediáticos y de contenidos publicitarios, pero las plataformas aquí estudiadas sí lo son. Por ejemplo, los canales de cable (y los servicios de streaming) suelen cobrar una cuota a los clientes que se abonan a sus canales o servicios, además de vender espacios publicitarios en ellos. Todas las principales redes sociales (por ejemplo, Instagram, Facebook, Twitter) son ejemplos modernos de estas empresas de medios mixtos, al igual que varios conglomerados mediáticos contemporáneos (por ejemplo, Disney).

Las páginas de redes sociales son el ejemplo más destacado de empresa contemporánea de medios mixtos. En contraste con los medios de comunicación tradicionales, gran parte del acceso a los contenidos de las redes es gratuito. Necesariamente, esto desplaza el meollo del beneficio económico, de las

personas, a las publicidades. Los anuncios están presentes en los contenidos audiovisuales y escritos de las redes sociales, tanto de forma descarada, como encubierta. Aparecen en las publicaciones de Instagram, en los tweets de Twitter, flotan en la parte superior de los resultados de las búsquedas en línea, e incluso tienen su propia pestaña en Gmail. Con un papel cada vez más importante por parte de los anuncios, las empresas tienen una necesidad renovada de comercialización entre los propios anunciantes. Para entender mejor el papel que desempeñan los anuncios en las redes sociales, hay que dilucidar mejor el propio concepto de publicidad.

El corazón de la publicidad es vender algo que la persona no ha pedido. Para que se produzcan esas ventas, los anuncios deben comprar y vender atención. Las ventas de atención, o anuncios, son un método de beneficio primordial para estas empresas. Para que este esfuerzo sea lo más eficaz posible, los anunciantes aprovechan los datos de los/as usuarios/as, que entran en las economías digitales de estas plataformas cada vez que navegan por internet, mucho antes de realizar cualquier compra. Para entender los beneficios y las prácticas publicitarias en estas plataformas, hay dos conceptos básicos que se aplican al consumidor, en cualquier plataforma. Las empresas venden un producto a un consumidor, o venden al consumidor como producto (Rahman-Jones, 2024). Vender un producto a un consumidor es la práctica tradicional de la publicidad explicada anteriormente. El anuncio en sí recomienda un producto que los anunciantes esperan convencer de que se quiere o se necesita. En este caso, la mercancía última es la atención. El segundo método, que funciona con bastante menos transparencia, convierte al consumidor en la mercancía. En este caso, la información que venden las empresas -como los rasgos, hábitos y comportamientos de los usuarios- es la máquina de obtener beneficios. En este sector del mercado, la mercancía son los datos.

Prácticas de recopilación de datos

Estas multinacionales utilizan la atención y los datos para generar beneficios. El intercambio relacionado con el beneficio a través de la atención puede denominarse economía de la atención. La economía de la atención es un concepto introducido por primera vez en la década de 1970 por Herbert Simon (1971), y ha sido ampliado y actualizado para la era de Internet por investigadores/as. Cuando las empresas venden la información que recopilan, contribuyen a la economía de los datos. La economía de los datos integra información en tiempo real y huellas digitales individuales para personalizar las experiencias en Internet (Shukla et al., 2023). La economía de los datos se nutre de la información generada por los usuarios de los sitios y plataformas.

Los detalles específicos de lo que se incluye cuando se recopilan los datos del usuario varían de una aplicación a otra y de un sitio a otro. Sin embargo, según las investigaciones, la mayoría de los espacios digitales, si no todos, recopilan arquetipos similares de información. Algunas empresas son conocidas por tener un nivel de datos más personal y vasto que otras. Meta, la empresa matriz de Instagram, es tristemente célebre por este tipo de prácticas. Un análisis de la política de privacidad de Instagram organizó su recopilación de datos así: "Información de cuenta y perfil", "Datos de interacción de contenido", "Información de dispositivo y conexión" (UpGrow, 2024). Estos términos parecen relativamente inocuos, pero incluyen una gran cantidad de información, desde tu dirección de correo electrónico, edad y sexo, hasta cuánto tiempo has visto un vídeo concreto, o la hora y ubicación precisas de la foto que subes a la plataforma.

Las etiquetas proporcionadas en la mayoría de las políticas de privacidad y los documentos de condiciones de servicio pueden entenderse generalmente por tres términos agregados. Recogen «Información Personal Identificable (IPI)», «Información de Comportamiento» y «Metadatos» (Singh, 2024). La IPI suele referirse a la información necesaria para crear una cuenta, como el nombre, los datos de contacto y, a veces, cosas como el sexo y la edad (Singh, 2024). La información sobre el comportamiento incluye los datos relacionados con la actividad individual en la plataforma (cómo y cuándo se utilizan los servicios, qué gusta o se comparte, qué cuentas siguen los usuarios, etc.) y los metadatos son datos sobre su dispositivo o patrones de navegación que no se incluirían en los datos sobre el comportamiento (Singh, 2024). Los datos de comportamiento y los metadatos suelen funcionar conjuntamente y pueden incluir cosas dentro y fuera de la aplicación o el sitio web. Información como los detalles de su dispositivo, ubicación, hora y fecha de las publicaciones, patrones de navegación (incluso en varias aplicaciones o sitios web) y, dependiendo de la aplicación, otros datos almacenados en el dispositivo que utiliza para acceder a la plataforma (Heiligenstein, 2023). Estos datos no se limitan a la plataforma o al sitio por el que navega el usuario en ese momento, sino que constituyen un perfil agregado sincronizado entre sitios y dispositivos, que utiliza detalles repetidos de la cuenta, direcciones IP, y hábitos de navegación para construir una visión de 360 grados de cada consumidor (Tau, 2024).

Un ejemplo de la profundidad de este alcance son los «datos de localización». Cuando una empresa se refiere a la recopilación de «datos de localización», un usuario medio podría suponer que un determinado servicio recopila datos de localización más o menos amplios, como su ciudad o Estado. En realidad, los datos de localización suelen ser muy específicos, refiriéndose a su ubicación en tiempo real determinada por direcciones IP o GPS (Tau, 2024). También puede abarcar datos de localización históricos o futuros,

dependiendo de las condiciones del servicio. También puede seguir recopilando dichos datos, lo que significa que un usuario puede aprobar que una aplicación específica utilice su ubicación durante una sola sesión, mientras que la aplicación puede rastrear su ubicación durante un periodo de tiempo mucho más largo: días, semanas o más (Klosowski, 2021). De este modo se garantiza que los datos que se venden sigan actualizándose y se ajusten mejor a la ubicación del usuario y, por tanto, a sus preferencias publicitarias (Keegan & Ng, 2021).

Los datos lo abarcan todo, y su recopilación no queda desaprovechada. Algunos de estos datos son necesarios para abrir y mantener una cuenta en las redes sociales, un proveedor de correo electrónico o muchas «suscripciones» a sitios web. Muchos de los datos recogidos son mucho más específicos y en mayor volumen de lo que un usuario medio puede captar. Un escrito de 2024 concluye que «comprender las explicaciones de la recopilación y el uso de datos personales suele requerir conocimientos especializados que escapan a la comprensión de la mayoría de los interesados» (Ding & Huang, 2024, p. 3). El lenguaje agradable y específico del sector utilizado en estos acuerdos de términos y condiciones es una elección estratégica por parte de las empresas, por varias razones.

Aunque amplia, esta lista sólo recoge los datos disponibles públicamente a través de diversos servicios en línea. Varias demandas y artículos han sugerido que, en algunos casos, la recopilación de datos podría ser mayor. En 2024, la Comisión Federal de Comercio (Federal Trade Commission, FTC) de EE. UU. impuso a Facebook una multa récord de 5.000 millones de dólares por su presunta violación de una orden de la FTC de 2012 al «engaño a los usuarios sobre su capacidad para controlar la privacidad de su información personal». A esto se une una denuncia del Departamento de Justicia en la que se alega que Facebook «utilizó repetidamente información y configuraciones engañosas para socavar las preferencias de privacidad de los usuarios» (Nguyen, 2024). Un año antes (en 2023), la Unión Europea impuso a Facebook una multa de 1.200 millones de euros por infracciones similares del derecho a la privacidad de los usuarios (EDPB, 2023). Google también tuvo una demanda en 2022 de 392 millones de dólares, por acusaciones de que la empresa «rastreaba a personas a través de sus dispositivos después de haber desactivado el seguimiento de la ubicación» (Allyn, 2022), lo que sugiere que, aunque las empresas desarrollen estas políticas de privacidad, su potencial de beneficio podría incentivar al incumplimiento de esos compromisos de privacidad.

Datos: comprados y vendidos

Byron Tau, en su libro *Means of Control: How the Hidden Alliance of Tech and government is creating a new American Surveillance State* (2024), profundiza en el entorno de la venta de datos. Explica las prácticas de «anonimización» de datos, algo que se hace antes de venderlos. Los datos se depuran de detalles protegidos legalmente antes de que los compradores los reciban. Cuando se «anonimizan» los datos de un usuario, su nombre se sustituye por un «identificador de usuario» compuesto de letras y números, mientras que todos los patrones y puntos de datos siguen siendo exactamente los mismos (Tau, 2024). Aunque así se eliminan los identificadores legales del perfil del usuario, a un anunciante le sirve de poco un nombre cuando dispone de todo el resto de la presencia en línea de un usuario (Tau, 2024). Cualquiera con acceso a esa misma información podría razonablemente digerir todas las preferencias y prácticas de una persona y, con tan solo tres puntos de localización GPS, descubrir rápidamente la información redactada (Tau, 2024).

Al comienzo de su libro, Tau pone como ejemplo una historia de este tipo en la que están implicados funcionarios del gobierno de Estados Unidos. En este ejemplo, destaca las vulnerabilidades técnicas relacionadas con los datos de localización «anonimizados» recopilados por Grindr, una aplicación de citas para hombres homosexuales. Los funcionarios de alto nivel podían ser localizados a través de los datos de localización en tiempo real que se compartían en la aplicación; una persona con pocos conocimientos de tecnología podía aprovecharse de esa localización compartida y conservar los datos de seguimiento de la ubicación en tiempo real incluso cuando el usuario cerraba la aplicación (Tau, 2024). Este ejemplo pone de manifiesto algunos de los amplios problemas de seguridad que plantea esta práctica, así como la compraventa de estos datos en general. Algunos sitios web disponen de «exclusión voluntaria» diseñada para dar a los usuarios alguna opción sobre la recopilación y el seguimiento de datos en el sitio y fuera de él, y Apple y Google ofrecen cada vez más opciones de exclusión voluntaria de seguimiento en sus dispositivos. Actualmente, un usuario no tiene garantizado el acceso a un determinado sitio o aplicación si decide rechazar el rastreo.

Una vez recopilados, los datos se venden. Esta industria se conoce como corretaje de datos. Los correderos de datos representan miles de millones de dólares de la cuota de mercado anual y, según los estudios de mercado, su influencia no hace más que crecer. Según Sharma y Chandola, «el tamaño del mercado mundial de intermediación de datos superó los 374.000 millones de dólares en 2023 y es probable que alcance casi los 672.000 millones de dólares en 2032» (2024). Se trata de un mercado que va mucho más allá de las grandes plataformas sociales. Los correderos de datos son anteriores a Internet y, aunque los detalles de los datos han cambiado drásticamente con el tiempo, los «datos» siguen siendo muy valorados por muchas industrias.

El corretaje de datos tiene una larga historia, entrelazada tanto con los anunciantes como con las industrias de seguridad. Antes de Internet, los intermediarios de datos estaban mucho más restringidos en cuanto a la información que podían recopilar. Los predecesores del corretaje de datos actual se reservaban a la información más básica, a menudo limitada al tipo de información que podía encontrarse en un censo. Las limitaciones de seguridad nacional y vigilancia también eran estrictas, limitadas a lo que se podía encontrar «en el exterior de un sobre» (Tau, 2024). Desde la época de la imprenta, los intermediarios de datos se han beneficiado al máximo al ofrecer la información más detallada y de mayor alcance posible, pero estaban limitados por lo que los individuos decidían compartir fuera de sus espacios privados. La evolución de la recopilación de datos y las actitudes hacia la privacidad cambiaron mucho tras los atentados del 11 de septiembre de 2001 a las Torres Gemelas, y desplazaron el límite de lo permitido.

Los anunciantes y las empresas quieren comercializar sus productos y servicios con la mayor eficacia posible en amplias franjas del mercado de consumo, y los intermediarios de datos ayudan en ese proceso. La profundidad de la información a la que tienen acceso las empresas privadas ha aumentado a pasos agigantados con la evolución de una Internet social. A medida que la gente comparte más detalles sobre sus vidas en una «plaza» a gran escala, las protecciones legales de décadas pasadas se han vuelto insuficientes. Las leyes modernas no han seguido el ritmo de la revolución de las redes sociales y, como resultado, los correderos de datos están vendiendo cada megabyte de datos que miles de millones de personas comparten sobre sí mismas y sus vidas, para que sean controlados por entes privados y gubernamentales por igual.

Los modernos correderos de datos venden en tiempo real todos los datos que pueden recopilar. La información recopilada mientras un usuario interactúa con una plataforma, una vez atribuida al «identificador de usuario» vinculado a su perfil digital, se envía instantáneamente a un montón de empresas que pagan mucho dinero por acceder a ella (Tau, 2024). En la mayoría de los casos, esta información se envía a un canal publicitario, donde el uso más pertinente de la información es contribuir al desarrollo de campañas publicitarias más eficaces y precisas. Esto significa que no sólo se valora la cantidad de datos, sino también su especificidad.

En la actualidad, la gama de datos «específicos» puede ir tan lejos como qué cuentas sigues, cuáles miras más, y dónde estás en un momento dado. Puede que la «anonimización» de estos datos no incluya tu nombre, pero garantiza que una empresa o un intermediario de datos pueda analizar toda tu presencia digital (en muchos casos, también en plataformas y sitios web) para, a continuación, elaborar los anuncios más eficaces y específicamente aplicables a toda tu identidad en línea. Las prácticas de marketing

contemporáneas sugieren que una empresa se beneficia de una audiencia altamente personalizada. Antes de ser un consumidor informado, hay que comprender el panorama de la intermediación de datos.

Aunque los servicios digitales se benefician en gran medida del intercambio de datos, también lo hacen del consiguiente aumento de la atención de los usuarios. Como dijo el Consejero Delegado de la empresa de tecnología de la atención Lumen, «la atención predice casi exactamente los beneficios» (Stewart, 2025). Las empresas pueden recibir una parte de las ventas de las campañas publicitarias exitosas en un sitio o plataforma determinados, y pueden cobrar tarifas más altas por el espacio publicitario cuando tienen mayores tasas de compromiso. En el ámbito de las redes sociales, el espionaje engloba el tiempo dedicado a utilizar e interactuar con una aplicación o servicio determinados (CLRN, 2024). Esta interacción es controlada y analizada, tanto interna como externamente, y se presenta como «datos del usuario» y, tanto en la economía de los datos como en la de la atención, los datos del usuario son relevantes y se utilizan.

El engagement (que podríamos traducir aquí como enganche, o compromiso de permanencia) es la métrica definitiva con la que se mide la economía de la atención. Desde el tiempo de navegación hasta el tiempo que los usuarios dedican a una publicación, o a compartirlo e interactuar con ella, el engagement engloba todos los datos de actividad (CLRN, 2024). Puede medirse en una sola cuenta, publicación, tema o cualquier otro margen. El engagement es también un factor importante a la hora de determinar las tarifas publicitarias de varias personas o cuentas que obtienen beneficios publicando en las plataformas. Las «tarifas de publicidad», se refieren a lo que cobra una determinada plataforma por sus distintos tipos de espacios publicitarios. Esto puede referirse tanto a empresas y plataformas como a «influencers» digitales, término utilizado para referirse a personas que obtienen beneficios compartiendo contenidos en la red. El lugar más común para los/as influencers es Instagram, Tiktok, Youtube y Facebook, las mismas plataformas que priorizan esta forma de compromiso y atención por parte de los usuarios. En ambos lados de este gran mercado de medios mixtos, hay un beneficio directo de mantener a los usuarios comprometidos en la plataforma.

Las tarifas publicitarias varían mucho según la entidad, y algunas celebridades tradicionales cobran supuestas sumas de más de un millón de dólares por una sola publicación en Instagram (Influencer Marketing Hub, 2025). Para anunciarse a través de las propias plataformas, las tarifas cambian en función del tipo de anuncio, la audiencia, y mucho más. Los analistas del sector estiman que las tarifas oscilan entre 0,40 y 0,70 dólares por clic en un solo anuncio (DeFazio, 2025). Los algoritmos específicos utilizados para determinar las tarifas publicitarias son secretos comerciales, y sólo pueden estimarse a partir de datos de dominio público. En cualquier caso, se mire por donde se mire, esta economía de la publicidad digital

es una economía con una enorme cantidad de dinero en circulación. El gasto mundial en publicidad digital superó los 790.000 millones de dólares en 2024 (Kemp, 2025), todo ello basado en la promesa de ojos y clics a través de la web. El proceso cíclico utiliza los ojos en los anuncios para generar ventas de productos y datos de los usuarios que prometen continuamente mejores ingresos por publicidad, independientemente de que hayan comprado o no un producto.

La mayoría de las personas cree que, a cambio de acceder de forma gratuita a una plataforma o sitio web, las empresas obtienen beneficios a través de la publicidad. Este fenómeno se conoce como «consentir o pagar» (Rahman-Jones, 2024), en referencia a la idea de pagar por el acceso o dar el consentimiento para el seguimiento de datos con fines lucrativos. Los consumidores pueden tener una comprensión general de este proceso de venta, pero la diferencia, entre las prácticas publicitarias tradicionales, y las prácticas publicitarias en las redes sociales, es enorme. La segmentación de los medios tradicionales es mucho menos individualizada, y el consumidor medio no tiene una idea clara de lo que se necesita para producir los anuncios cuidadosamente seleccionados que ve en sus redes sociales. Estas empresas se benefician en gran medida de que los consumidores no comprendan la cantidad de datos que se necesitan para generar ese tipo de anuncios. En tiempo real, se selecciona un anuncio para ellos como resultado del acceso de varias empresas a una gran cantidad de información personal y hábitos digitales. El malentendido es un problema importante. Sin embargo, el control que tienen las empresas sobre la forma en que los usuarios gastan su dinero y su tiempo es una amenaza aún mayor.

El consumidor desinformado

Como se ha mencionado anteriormente, las empresas de servicios digitales, en general, obtienen beneficios al aumentar el tiempo y las actividades de interacción de los usuarios en sus plataformas. Dentro del sector, las métricas de interacción se consideran uno de los principales factores determinantes para que tanto las empresas como los/as influencers puedan aumentar sus tarifas para diversos tipos de anuncios (DeFazio, 2025). Esto crea una máquina auto-sostenible en la que más personas publican y anuncian, lo que aumenta los beneficios y el movimiento de este mercado en su conjunto. Las empresas de redes sociales disponen de datos que explican qué tipo de publicaciones y contenidos atraen a los consumidores en mayor medida. Todos los que se benefician de cualquier tipo de publicidad que circula en línea se benefician de estadísticas mejores, más detalladas y precisas sobre los usuarios. Todas las partes del lado lucrativo de la ecuación -que, cabe destacar, no incluye a los usuarios- buscan continuamente formas de aumentar sus beneficios, lo que incentiva a las empresas no solo a obtener, sino también a presentar y compartir versiones más detalladas de los datos de los usuarios. Esto fue, en parte,

un elemento importante del escándalo de Cambridge Analytica, a finales de la década de 2010 (Chomanski, 2025).

El acontecimiento central del escándalo de Cambridge Analytica fue el descubrimiento de que, en colaboración con Facebook, Cambridge Analytica, una empresa privada contratada, podía influir en la actividad de los usuarios en las redes sociales de forma tan drástica que fue capaz de influir con éxito en múltiples elecciones y votaciones en todo el mundo. Un artículo de *The Guardian* cita a un antiguo empleado de Cambridge Analytica que afirma:

La empresa podía crear anuncios que nadie más podía hacer: un demócrata neurótico, extrovertido y agradable podía ser el objetivo de un mensaje radicalmente diferente al de uno emocionalmente estable, introvertido e intelectual, cada uno diseñado para suprimir su intención de voto, incluso si los mismos mensajes, intercambiados, tuvieran el efecto contrario. (Hern, 2018).

La idea de que, con suficientes puntos de datos (cualquier información que se pueda obtener de cómo usas Internet), una empresa puede crear un mensaje específico y hábil que te incite a actuar de una manera concreta puede resultar intimidante. También es una realidad probada. El ejemplo de Cambridge Analytica nos recuerda que este acceso nos desconocido, y con ello, no lo entendemos, y no cuenta con la aprobación del público cuando los usuarios están debidamente informados. Un artículo de CBS News publicado tras el estallido del escándalo cita a un usuario que afirma: «Facebook me ha dado cada vez más razones para no confiar en ellos»; explica que ha reducido su uso de unos 30 minutos diarios a unos 10 minutos cada dos días y que «estaría encantado de dejarlo por completo si surgiera una alternativa viable» (CBS, 2018).

La participación de Facebook (Meta) en este engaño fue significativa por varias razones. Desde el punto de vista político, este escándalo demuestra la gran influencia y el cambio que se puede ejercer con la información personal que se compra y se vende en Internet cada día. Aunque la influencia política y cultural no se limita en absoluto a las elecciones presidenciales estadounidenses de 2016, la investigación y los datos de este evento son muy amplios y constituyen un claro ejemplo. En un análisis realizado en la Universidad de Carolina del Norte en Chapel Hill, los investigadores llevaron a cabo entrevistas durante el ciclo electoral. Descubrieron que «estas empresas [Facebook, Google, Microsoft, Twitter] son intermediarios más activos en la política electoral estadounidense de lo que se reconoce convencionalmente en la literatura» (Kreiss y McGregor, 2017). Esta confabulación, especialmente en el ejemplo de las elecciones estadounidenses de 2016, no solo fue muy eficaz para las campañas en las que

más participaron, sino que también resultó beneficiosa para sus resultados finales. Los empleados de estos diversos sitios web que trabajaron, en efecto, para las campañas políticas, proporcionaron un fuerte retorno de la inversión: «Estos empleados de las empresas tecnológicas, a su vez, generaron mayores beneficios tanto para estas empresas como para las campañas... Para las empresas tecnológicas, esto significó más ingresos» (Kreiss y McGregor, 2017). El aumento de los ingresos es la máxima prioridad para estas empresas tecnológicas, incluso si ello supone desinformar a los usuarios.

La participación en la política electoral aumentó con el tiempo, lo que, junto con las ventas a diversos corredores de datos, creó un entorno propicio para que prosperara una empresa como Cambridge Analytica. Se ha señalado que Facebook era consciente del aumento de la polarización y la volatilidad en su sitio web y en el panorama general, a menudo como resultado de estos contenidos profundamente segmentados (Horwitz, 2023). Sin embargo, Facebook no hizo ningún intento serio por frenar estas preocupaciones después de tener conocimiento de ellas. De hecho, algunas de estas actividades contribuyeron a aumentar la participación en la plataforma (Horwitz, 2023). Dada la importancia de la participación como indicador crítico, muchas empresas pudieron presentar esta polarización y disonancia como un éxito, citando el aumento de la circulación de anuncios, la participación de los usuarios y las ventas de anuncios en los períodos de ventas correspondientes (Team, 2017).

Si bien las consecuencias del trabajo de Cambridge Analytica y otras empresas similares son significativas y generalizadas, aquí revisten especial importancia porque están relacionadas con el núcleo de este trabajo: el consumidor desinformado. El concepto de «desinformado» es muy anterior a Internet, tiene muchas aplicaciones, pero se ha estudiado mucho en el ámbito de la política. James Kuklinski, politólogo, fue pionero en profundizar en ello, explicando que, para estar informadas, las personas deben tener creencias basadas en hechos sobre un tema, y esas creencias deben ser precisas; si las personas no tienen creencias basadas en hechos, están desinformadas (Kuklinski et al., 2000). Elina Lindgren, una politóloga más contemporánea, establece una distinción importante con respecto a la realidad de la naturaleza humana: tomar decisiones basadas en falacias. Afirma que «esta división de los ciudadanos en informados y desinformados ignora el hecho de que las personas pueden creer en la respuesta equivocada, algo que debe considerarse distinto de la falta de conocimientos y creencias» (Lindgren et al., 2022). Estos conceptos se han debatido ampliamente en contextos políticos, pero no se puede subestimar su relevancia para la economía de la atención y el consumo.

Las consecuencias de que un usuario no esté informado son graves. Los usuarios deben navegar por un ámbito social cada vez más relevante sin comprender su función real. Los datos del Pew Research Center

explican que «el público afirma cada vez más que no entiende lo que las empresas hacen con sus datos. Alrededor del 67% afirma que entiende poco o nada sobre lo que las empresas hacen con sus datos personales» (McClain et al., 2023a). Los consumidores no solo sienten que no controlan el uso que se hace de su información, sino que, a menudo, esa falta de comprensión influye en la forma en que interactúan con las plataformas. Un estudio, realizado en 2021 por Sigitas Urbanavicius et al., explicaba que «la disposición [de los usuarios de las redes sociales] a revelar datos personales se veía afectada negativamente por la percepción de falta de control» sobre los datos recopilados (p. 82). Existe una correlación entre el aumento de la concienciación sobre las prácticas de recopilación de datos y la percepción de pérdida de control. Esa falta de control sobre la recopilación de sus propios datos a menudo lleva a los usuarios a minimizar su divulgación, si se les da la oportunidad. Una encuesta de Consumer Reports de 2024 respalda esta idea, ya que revelaba que el 78% de los encuestados estaba a favor de la regulación y la limitación de la recopilación de datos por parte de diversas empresas (Medintz, 2024).

En los últimos años, especialmente a raíz de los escándalos y demandas judiciales en torno al uso que estos gigantes tecnológicos hacen de los datos de los usuarios, ha aumentado la desconfianza hacia las empresas (y hacia muchos gobiernos). A medida que siguen circulando noticias e información sobre diversos actores que gestionan de forma inadecuada los datos personales, la confianza sigue disminuyendo en todos los grupos de edad, afiliaciones políticas e identidades. Entre 2019 y 2023, observamos un aumento de siete o más puntos porcentuales en varias preguntas centradas en la confianza, incluida la falta de confianza de los estadounidenses en la forma en que el gobierno utiliza sus datos, y lo poco que entienden sobre cómo se utilizan (McClain et al., 2023a). El desarrollo conjunto de estos sentimientos sugiere que, cuando se tiene una comprensión verdadera y justa de cómo se utiliza y se comparte su información, las personas confían menos en las empresas y plataformas que reclaman su información. Las personas que están mejor informadas sobre el posible uso indebido de los datos personales tienen más probabilidades de optar por no participar y decidir no revelar dicha información. Un estudio de 2020 explica que «a la hora de decidir si divulgar información, las personas tienen en cuenta la cantidad de datos privados que se recopilan» (Lee y Yuan, 2020).

Cuando los usuarios de todos los grupos de edad comprenden mejor las prácticas maliciosas, su desilusión aumenta. Tras el escándalo de Cambridge Analytica, «Facebook perdió 50000 millones de dólares en capitalización bursátil en dos días» (Richter, 2019). La rápida difusión de esta información, tanto por parte de periodistas y medios de comunicación, como de particulares, permitió a los usuarios hacerse una idea más clara de su entorno digital. Casi de inmediato, Facebook perdió el favor del público y, en consecuencia,

los fondos públicos. Como muestra este ejemplo, un consumidor informado es una amenaza para los beneficios de estos gigantes de los medios de comunicación.

Esta discrepancia también se refleja en la correlación entre los lugares donde existe la mejor legislación en materia de privacidad, y los beneficios posteriores de esas regiones. Los márgenes de beneficio de los usuarios estadounidenses son drásticamente superiores a los de los usuarios de Europa. El 46% de los ingresos totales de Alphabet, la empresa matriz de Google, proviene únicamente de Estados Unidos, y el 44% de los casi 115.000 millones de dólares de ingresos publicitarios de Meta proviene de Estados Unidos y Canadá, según Visual Capitalist (Ang, 2022). Los Estados Unidos son el mayor mercado de beneficios para estas empresas, y también tienen la legislación más débil en materia de protección de datos, en comparación con la UE. La Unión Europea ha implementado el Reglamento General de Protección de Datos (RGPD) desde 2018 y, según la UE, es «la ley de privacidad y seguridad más estricta del mundo» (*The General Data Protection Regulation, 2024 -GDPR-*). Este reglamento aumenta el control que los ciudadanos tienen sobre sus datos, y obliga a las empresas que interactúan con usuarios de la UE. Es fundamental destacar que este reglamento exige el «derecho al olvido», es decir, el derecho de las personas a solicitar que se eliminen sus datos personales, algo que no está garantizado en todas partes. En Estados Unidos, la legislación no es comparable y, como resultado, las empresas tienen mucho más acceso a los datos en línea de los estadounidenses.

También está la cuestión de las políticas de privacidad de los propios sitios web y empresas. Un informe del *New York Times* ofrece una síntesis de varias políticas de privacidad, que también se han incluido en Lexile, un software diseñado para comprender los niveles de lectura de los textos. Litman-Navarro explica:

Para tener éxito en la universidad, las personas deben comprender textos con una puntuación de 1300. Las personas que ejercen profesiones liberales, como médicos y abogados, deben ser capaces de comprender materiales con puntuaciones de 1440, mientras que los alumnos de noveno curso deben comprender textos con puntuaciones superiores a 1050 para estar preparados para la universidad o una carrera profesional cuando se gradúen. Muchas políticas de privacidad superan estos estándares. (2019).

Esto coincide con informes que indican que los usuarios no comprenden lo que están aceptando en dichas políticas de privacidad. El Dr. King, director de privacidad del consumidor del Centro para Internet y Sociedad de Stanford, es citado por el *Times* diciendo: «Estos documentos fueron creados por abogados, para abogados. Nunca se crearon como una herramienta para el consumidor» (Litman-Navarro, 2019). La

jerga legal y los bajos índices de legibilidad que abundan en estas políticas dificultan la comprensión de las mismas por parte de los consumidores.

Aparte de la cuestión de la claridad, la mayoría de los usuarios no leen los términos y condiciones en absoluto. El tono que evocan los términos utilizados por estas empresas no pretende alarmar al usuario medio, sino ayudar a mantener una reacción ecuánime por parte de los usuarios *en caso de que* lean los términos que están aceptando. No leen las condiciones de lo que utilizan. Nili Steinfeld explica que, cuando los usuarios tienen la opción de aceptar los términos y condiciones de un sitio web sin leer la política, suelen renunciar a leer el documento... Incluso cuando los usuarios deciden hacer clic en un enlace no obligatorio para leer la política, dedican mucho menos tiempo y esfuerzo a leer el documento (2016).

Estas políticas también están diseñadas, en general, para transmitir información precisa desde el punto de vista técnico, de tal manera que, si un usuario no tiene un buen dominio de la terminología, es poco probable que comprenda el alcance completo del término. Esto solo agrava el problema de la falta de información del consumidor. Los usuarios se ven constantemente bombardeados con políticas de privacidad que son deliberadamente vagas y difíciles de entender (Parker, 2024). Con el tiempo, los usuarios son menos propensos a leer las políticas y más propensos a confundirse si intentan leerlas. En el documento, sin embargo, sigue habiendo misterio. El lenguaje ambiguo está diseñado para «proteger a las empresas» (Litman-Navarro, 2019), y proporciona un margen legal a las corporaciones que están detrás de estos servicios, otorgándoles un amplio acceso y un control limitado a los usuarios. Cuanto menos específico es el lenguaje, menos probable es que las empresas reciban reacciones negativas, ya sea a nivel legal o público.

Si bien el GDPR -mencionado antes- de la UE tuvo un impacto positivo en algunas políticas de privacidad, aún queda mucho por mejorar. Sigue existiendo el problema de la falta de comprensión por parte de los usuarios en lo que respecta a los datos que se recopilan y cómo se utilizan. En concreto, sobre la política de privacidad de Google, *The Times* afirma que

la política se hizo más legible a costa de la brevedad tras la introducción del Reglamento General de Protección de Datos... El reglamento incluye una cláusula que exige que las políticas de privacidad se presenten de forma «concisa, transparente e inteligible, utilizando un lenguaje claro y sencillo». (Litman-Navarro, 2019).

No ayuda el hecho de que, al consultar las políticas directamente en la fuente, el usuario pueda acabar sin comprender bien la política que ha aceptado. Un estudio de 2024 sobre la eficacia de las políticas de privacidad en línea explica que «aunque las personas puedan acceder fácilmente a la información, el alto

coste que supone comprenderla puede impedirles tomar decisiones informadas» (Ding y Huang, 2024, p. 13). Las empresas se ven favorecidas cuando los usuarios buscan más información «directamente en la fuente» como consecuencia de dicha baja comprensión, y del alto tiempo que requiere leer las políticas en su totalidad. Ding y Huang se refieren a esto afirmando que

Los interesados deben dedicar mucho tiempo a leer todas las políticas de privacidad que deben aceptar... El contenido de las políticas de privacidad es demasiado complejo para que lo entiendan los particulares. Comprender las explicaciones sobre la recogida y el uso de los datos personales suele requerir conocimientos especializados que escapan a la comprensión de la mayoría de los interesados. (2024, p. 3).

A menudo, la información de origen, si se analiza con un nivel de comprensión medio, deja al usuario con una idea muy básica del consentimiento que está otorgando. A los usuarios no les resulta fácil comprender cómo se utiliza su tiempo y su información en Internet, y las empresas se benefician de ello. Cuando los usuarios se informan, su comportamiento cambia. Un estudio anterior del Pew Research Center ofrece un ejemplo:

Después de que Edward Snowden, contratista de la Agencia de Seguridad Nacional, revelara detalles sobre los programas de vigilancia gubernamental iniciados en 2013, el 30% de los adultos afirmó haber tomado medidas para ocultar o proteger su información y el 22% declaró haber cambiado su comportamiento en Internet con el fin de minimizar la posibilidad de ser detectados. (Rainie, 2018).

Otros estudios, como el realizado por Christine Prince en 2018, concluyen que «las personas que están mejor informadas sobre el posible uso indebido de los datos personales tienen más probabilidades de optar por no revelar dicha información» (p. 30). En el panorama económico del comercio de datos, la disminución de la divulgación de información por parte de los usuarios tiene un impacto económico negativo en las empresas de redes sociales.

Las poblaciones más informadas son las que tienden a tomar las medidas más enérgicas para proteger su privacidad. En todas las investigaciones relacionadas con la privacidad de los datos realizadas por Pew, las poblaciones más jóvenes están sistemáticamente mejor informadas y tienen una mayor confianza en su comprensión del panorama de la privacidad digital, en comparación con las generaciones mayores. Se trata de las mismas poblaciones que presentan el porcentaje más alto de medidas cuando se trata de dar prioridad a la privacidad de sus datos. Esto se observa en la investigación del Pew Research Center,

El 76% de los usuarios de redes sociales menores de 50 años afirma haber cambiado la configuración de privacidad de sus perfiles en redes sociales. El 49% afirma haber utilizado un navegador o motor de búsqueda que no rastrea sus actividades. El 42% afirma haber utilizado aplicaciones o servicios de mensajería que cifran sus comunicaciones privadas. (McClain et al., 2023b).

La investigación de Lee y Huang coincide con esta afirmación, y señala que los estudiantes utilizaron diversas estrategias para gestionar su privacidad, entre ellas limitar el acceso y la información de su perfil mediante la exclusión de datos y decisiones estratégicas sobre quiénes eran sus amigos (2020). Los jóvenes tienen más familiaridad, comprensión y prácticas de privacidad en línea.

Además de la disminución de la confianza de los usuarios, las empresas han sufrido pérdidas económicas a raíz de los escándalos relacionados con la recopilación de datos y la privacidad. Ha habido un aumento tanto de los usuarios, como de los gobiernos, que buscan una mayor protección y privacidad en su navegación, así como una creciente desilusión con el panorama actual de las redes sociales. Una encuesta de Gartner, realizada a 263 consumidores, entre julio y agosto de 2023, reveló que el 53% de los consumidores cree que el estado actual de las redes sociales ha empeorado en comparación con el año anterior, o con hace cinco años. Las principales razones de este deterioro percibido fueron la difusión de información errónea, las bases de usuarios tóxicas, y la prevalencia de los bots. Se esperaba que la percepción de deterioro de la calidad de las plataformas de redes sociales llevara al 50% de los consumidores a abandonar o limitar significativamente sus interacciones con las redes sociales para 2025 (Gartner, 2023). La disminución del uso de estas plataformas es perjudicial para los ingresos reales de estas empresas, un destino que se evita siempre que es posible, incluso si eso significa sembrar información polarizadora o «mala» para mantener la adicción.

Con las amenazas de la legislación y la disminución del número de usuarios, es fácil imaginar que las empresas están más desesperadas que antes por mantener estos altos niveles de beneficios y compromiso. Tras los escándalos y la agitación política, y con muchos usuarios buscando restar prioridad al uso de las redes sociales, las empresas mencionadas aquí se ven sometidas a una presión cada vez mayor para mantener un entorno aceptable para sus clientes finales: los anunciantes. Si el uso disminuye, la economía de los medios mixtos se marchita. Hay menos datos que vender y menos compromiso con los anuncios. Mientras las redes sociales han estado operando en la oscuridad, los usuarios han estado luchando contra su desconocimiento. Los usuarios quieren más opciones y más transparencia, incluso si eso perjudica a los anunciantes.

Este mismo año (2025), Meta ha llevado a cabo una revisión completa de su política de privacidad, uno de cuyos aspectos fundamentales es la mejora de la claridad (UMA Technology, 2025). Según UMA Technology, Meta pretende «recuperar la confianza de los usuarios, que se ha visto mermada tras diversos escándalos y presiones normativas» (2025). No es fácil para los usuarios comprender cómo se utiliza su tiempo y su información en Internet, y las empresas se benefician de ello. Estos cambios tienen un coste, ya que estas empresas se enfrentan a multas cuantiosas y ramificaciones legales por este «comercio en la oscuridad». Sus beneficios eran mejores antes de que los usuarios quisieran comprender mejor sus prácticas, y ahora se están adaptando a las expectativas de diversos gobiernos en materia de divulgación y cumplimiento de las políticas.

Conclusión

Parte del éxito de estas empresas radica en dificultar que el consumidor comprenda realmente su entorno digital. La ocultación de información se produce en línea de muchas maneras. En primer lugar, las políticas y prácticas de estas empresas son vagas y poco transparentes. Esto impide de forma inherente que los consumidores menos decididos comprendan en profundidad el funcionamiento de la empresa tal y como lo definen ellos mismos. También existe una gran afluencia de datos entre las distintas plataformas, lo que satura y abruma al consumidor medio. Esto contribuye a disuadir a muchos consumidores de investigar activamente el funcionamiento de sus aplicaciones favoritas. Por último, se ha demostrado que las empresas actúan al margen de los términos y condiciones establecidos por sus propios organismos internos y externos. Estos ejemplos generales permiten comprender claramente las dificultades a las que se enfrenta un consumidor que desea estar informado. La tarea se ve dificultada por el flujo interminable de cambios en las plataformas y las políticas. Estos son elementos fundamentales de los modelos de negocio utilizados por estas empresas de redes sociales.

Este artículo aclara la verdad sobre el incentivo que tienen estas empresas para mantener a los consumidores con un conocimiento mínimo sobre cómo se recopilan, compran y venden sus datos. Cuanto más presentes están los usuarios -más comprometidos- en las plataformas y servicios que ofrecen estas empresas, mayores son sus márgenes de beneficio. Pueden vender publicidad más cara y en mayor volumen. Pueden vender datos cada vez más precisos a más y más corredores de datos. Cuando los consumidores no están informados sobre cómo se utilizan y venden estos datos, las empresas, en efecto, realizan sus transacciones en la oscuridad. Los usuarios interactúan a un ritmo elevado, sin comprender apenas cómo generan sus beneficios estas empresas.

Cuando los usuarios están más informados, tienden a querer derechos y procedimientos diferentes para sus datos y su privacidad. Cuando existe una sólida comprensión de cómo se recopilan sus datos, los usuarios tienden a intentar ajustar la configuración de privacidad en sus espacios digitales. Cuando los usuarios comprenden cómo se venden sus datos, tienden a limitar la recopilación de datos siempre que es posible. Lo que es más amenazador, limitan su uso. A medida que más escándalos y conocimiento sobre la realidad de la vigilancia de datos y las violaciones de la privacidad llegan a la opinión pública, crece el cansancio y cae la confianza entre los usuarios.

La mayor amenaza para estas empresas es que acabe la falta de atención, y que las personas se preocupen por sus datos. En última instancia, a estas empresas les beneficia que los usuarios no comprendan lo que están haciendo al otro lado de sus algoritmos. Este problema no es nuevo, sino que se ha agravado con el tiempo, a pesar de los intentos gubernamentales e institucionales por frenar la recopilación de datos. La conclusión de esta investigación es que, mientras las empresas sigan obteniendo beneficios, los propios usuarios deben tomar las riendas de su vida digital, en interés propio y colectivo.

Bibliografía

- Allyn, B. (2022, November 14). Google pays nearly \$392 million to settle sweeping location-tracking case. *NPR*. <https://www.npr.org/2022/11/14/1136521305/google-settlement-location-tracking-data-privacy>
- Anderson, J., & Lee Rainie. (2017, October 19). *The Future of Truth and Misinformation Online*. Pew Research Center. <https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/>
- Ang, C. (2022, April 25). How Do Big Tech Giants Make Their Billions? *Visual Capitalist*. <https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2022/>
- CBS/AP. (2018). Can Facebook restore public trust after Cambridge Analytica scandal? *CBS News*. <https://www.cbsnews.com/news/facebook-cambridge-analytica-restore-public-trust-after-privacy-scandal/>
- Chomanski, B. (2025). The challenge of regulating digital privacy. *Critical Review of International Social and Political Philosophy*, 0, 1-25. <https://doi.org/10.1080/13698230.2025.2478725>
- CLRN. (2024, December 9). What are social media engagements? *California Learning Resource Network*. <https://www.clrn.org/what-are-social-media-engagements/>
- DeFazio, A. (2025, April 4). How Much Do Instagram Ads Cost? (+How to Make the Most of Your Budget). *WordStream*. <https://www.wordstream.com/blog/ws/2021/02/08/instagram-ads-cost>

- Ding, X., & Huang, H. (2024). For whom is privacy policy written? A new understanding of privacy policies. *Computer Law & Security Review*, 55, 1-13. <https://doi.org/10.1016/j.clsr.2024.106072>
- EDPB. (2023, May 22). 1.2 billion Euro fine for Facebook as a result of EDPB binding decision. *European Data Protection Board*. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en
- Fuchs, C. (2020). *Communication and Capitalism. A critical theory*. University of Westminster Press. <https://doi.org/10.2307/j.ctv12fw7t5>
- Gartner Inc. (2023, December 18). Gartner Predicts 50% of Consumers Will Significantly Limit Their Interactions with Social Media by 2025. *Gartner*. <https://www.gartner.com/en/newsroom/press-releases/2023-12-14-gartner-predicts-fifty-percent-of-consumers-will-significantly-limit-their-interactions-with-social-media-by-2025>
- Heiligenstein, M. (2023, August 8). How companies track you online – the definitive guide. *Firewall Times*. <https://firewalltimes.com/how-companies-track-you-online/>
- Hern, A. (2018, May 6). Cambridge Analytica: How did it turn clicks into votes? *The Guardian*. <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>
- Horwitz, J. (2023). *Broken code: Inside Facebook and the fight to expose its harmful secrets*. Doubleday.
- Influencer Marketing Hub. (2025, March 21). 20 of Instagram's highest paid stars in 2024. *Influencer Marketing Hub*. <https://influencermarketinghub.com/instagram-highest-paid/>
- Keegan, J., & Ng, A. (2021, September 30). There's a multibillion-dollar market for your phone's location data. *The Markup*. <https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data>
- Kemp, S. (2025, March 23). Digital 2025: Global Overview Report - DataReportal – Global Digital Insights. *DataReportal*. <https://datareportal.com/reports/digital-2025-global-overview-report>
- Klosowski, T. (2021, May 6). We checked 250 iphone apps-this is how they're tracking you. *The New York Times*. <https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/>
- Kreiss, D., & McGregor, S. C. (2017). Technology firms shape political communication: The work of Microsoft, Facebook, Twitter, and google with campaigns during the 2016 U.S. presidential cycle. *Political Communication*, 35(2), 155–177. <https://doi.org/10.1080/10584609.2017.1364814>
- Kuklinski, J. H., Quirk, P. J., Jerit, J., Schwieder, D. and Rich, R. F. (2000). Misinformation and the Currency of Democratic Citizenship. *The Journal of Politics*, 62(3), 790-816. <https://www.jstor.org/stable/2647960>
- Lee, Y.-H. and Yuan, C. W. (2020). The Privacy Calculus of "Friending" Across Multiple Social Media Platforms. *Social Media + Society*, 6(2). <https://doi.org/10.1177/2056305120928478>

- Lindgren, E., Damstra, A., Strömbäck, J., Tsafati, Y., Vliegenthart, R. and Boomgaarden, H. (2022). *Knowledge Resistance in High-Choice Information Environments*. Routledge. <https://doi.org/10.4324/9781003111474-10>
- Litman-Navarro, K. (2019, June 12). We read 150 privacy policies. they were an incomprehensible disaster. *The New York Times*. <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>
- McClain, C., Faverio, M., Anderson, M. and Park, E. (2023a, October 18). 1. Views of data privacy risks, personal data and Digital Privacy Laws. *Pew Research Center*. <https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/>
- McClain, C., Faverio, M., Anderson, M. and Park, E. (2023b, October 18). How Americans View Data Privacy. *Pew Research Center*. <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>
- Medintz, S. (2024, November 20). Americans Want Much More Online Privacy Protection Than They're Getting. *Consumer Reports*. <https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306/>
- Nguyen, S. (2024, August 20). FTC imposes \$5 billion penalty and sweeping new privacy restrictions on Facebook. *Federal Trade Commission*. <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>
- Parker, K. D. (2024, August 12). The hidden dangers of privacy laws like the GDPR and CCPA. *Forbes*. <https://www.forbes.com/councils/forbestechcouncil/2020/11/25/the-hidden-dangers-of-privacy-laws-like-the-gdpr-and-ccpa/>
- Prince, C. (2018). Do consumers want to control their personal data? empirical evidence. *International Journal of Human-Computer Studies*, 110, 21-32. <https://doi.org/10.1016/j.ijhcs.2017.10.003>
- Rahman-Jones, I. (2024, August 23). Should you have to pay for online privacy? *BBC News*. <https://www.bbc.co.uk/news/articles/c93599ejdeno>
- Rainie, L. (2018, March 27). Americans' complicated feelings about social media in an era of privacy concerns. *Pew Research Center*. <https://www.pewresearch.org/short-reads/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/>
- Richter, F. (2019, May 11). Wall Street Has Moved On From Cambridge Analytica Scandal. *Statista*. <https://www.statista.com/chart/13822/facebook-share-price/>
- Sharma, R. and Chandola, V. (2024). Data broker market. *Dataintelo*. <https://dataintelo.com/report/data-broker-market>

- Shukla, S., Bisht, K., Tiwari, K. and Bashir, S. (2023). *Data Economy in the Digital Age*. Springer.
https://doi.org/10.1007/978-981-99-7677-5_1
- Simon, H. A. (1971). Designing Organizations for and Information-Rich World. In M. Greenberger (Ed.), *Computers, communications, and the public interest* (pp. 37-72). Johns Hopkins University Press.
<https://gwern.net/doc/design/1971-simon.pdf>
- Singh, B. (2024, October 11). The Privacy Policy of Social Media Platforms. *The Law Communicants*.
<https://thelawcommunicants.com/the-privacy-policy-of-social-media-platforms/>
- Steinfeld, N. (2016). "I agree to the terms and conditions": (how) do users read privacy policies online? an eye-tracking experiment. *Computers in Human Behavior*, 55, 992-1000.
<https://doi.org/10.1016/j.chb.2015.09.038>
- Stewart, T. (2025, April 3). Driving engagement: How attention delivers profits. *New Digital Age*.
<https://newdigitalage.co/advertising/attention-profits-uber-advertising-lumen-research-paul-wright-mike-follett/>
- Tau, B. (2024). *Means of control: How the Hidden Alliance of Tech and government is creating a new American Surveillance State*. Crown.
- Team, T. (2017, October 30). Facebook's Strong Ad Revenue Growth to Continue. *Forbes*.
<https://www.forbes.com/sites/greatspeculations/2017/10/30/facebook-s-strong-ad-revenue-growth-to-continue/>
- The General Data Protection Regulation - Consilium. (2024, June 13).
<https://www.consilium.europa.eu/en/policies/data-protection-regulation/>
- Tremblay, A. (2024, February 27). 2024: The Year of Disengagement from Social Media. Tink.
<https://www.tink.ca/en/insights/2024-year-disengagement-social-media>
- UMATechnology. (2025, January 27). Meta Rolls Out Privacy Policy Update for Instagram and facebook. *UMA Technology*. <https://umatechnology.org/meta-rolls-out-privacy-policy-update-for-instagram-and-facebook/>
- UpGrow. (2024, October 25). What data does Instagram collect. *UpGrow*.
<https://www.upgrow.com/blog/instagram-data>
- Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V., & Skare, V. (2021). From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory. *Journal of Business Research*, 136, 76-85.
<https://doi.org/10.1016/j.jbusres.2021.07.031>