MSMK University College

Tech and Employment: Empowering Tomorrow's Talent

#8

Huellas digitales y Grandes Empresas

MSMK Magazine

8.ª Edición - Huellas digitales y grandes empresas

En esta edición de MSMK Magazine, exploramos cómo cada clic, búsqueda y transacción se convierte en una pieza más del inmenso mapa de datos que las grandes empresas construyen sobre nosotros. A lo largo de la revista, se analiza el impacto real de la huella digital y la economía de la vigilancia, examinando cómo compañías tecnológicas convierten nuestro comportamiento cotidiano en su activo más valioso.

CONTENIDO

01 PÁG 05 **EL PERFIL INVISIBLE:CÓMO LAS EMPRESAS CONSTRUYEN TU IDENTIDAD DIGITAL**
AXEL BRAOJOS PEREZ

02 PÁG 07 **EL DISFRAZ DE LA PUBLICIDAD**
DAVID LANCHEROS IPUS

03 PÁG 09 **CURRICULUM SHADOW**
GABRIEL FALCAO SANTOS

04 PÁG 11 ***BROWSER FINGERPRINTING*: CÓMO TE IDENTIFICAN SIN QUE LO SEPAS**
HUGO HERNÁNDEZ MORENO

05 PÁG 13 **THE DATA MONOPOLY OF BIG TECH**
IGNACIO QUIROZ COSCOLLANO

06 PÁG 16 **EL FIN DEL ANONIMATO: QUIÉN COMPRA Y VENDE TU RASTRO EN INTERNET**
JORGE MADRID VALNICKAS

07 PÁG 19 **LA HUELLA DIGITAL EN LA CONTRATACIÓN LABORAL**
PABLO DEL RÍO MARTÍNEZ

08 PÁG 22 **HUELLAS DIGITALES Y GRANDES EMPRESAS: EL RASTRO INVISIBLE DEL PODER CORPORATIVO**
PABLO GARCÍA OLLERO

09 PÁG 26 **EL ALGORITMO PSICOLÓGICO: CÓMO TU HUELLA DIGITAL PREDICE TU SOLVENCIA Y PERPETÚA LA DESIGUALDAD**
RUBÉN VALVERDE ROMERO

CONTENIDO

10 PÁG 28 **YOUR PRIVACY AS A PRODUCT: THE HIDDEN BUSINESS OF DIGITAL FOOTPRINTS**
SANDRA ESPIÑEIRA BRICEÑO

11 PÁG 30 **LA HUELLA DIGITAL DESDE LA INFANCIA: CRECER EN INTERNET ANTES DE APRENDER A PROTEGERSE**
SANDRA GUTIERREZ DE TENA

12 PÁG 33 **TU HUELLA EN INTERNET VALE DINERO Y NO ES PARA TI**
VICTOR ASUNCIÓN

AXEL BRAOJOS PEREZ

El perfil invisible: **Cómo las empresas construyen identidad digital**

La vida cotidiana se desarrolla en un entorno crecientemente conectado: búsquedas en la web, compras en línea, uso de aplicaciones, compartición de ubicación y participación en redes sociales generan rastros continuos de información. Estas trazas —a menudo producidas de forma automática y sin plena conciencia— constituyen una huella digital que puede ser almacenada, correlacionada y reutilizada por múltiples actores del ecosistema digital.

En este contexto, las empresas emplean algoritmos avanzados y técnicas de Inteligencia Artificial para transformar datos dispersos en perfiles digitales que representan hábitos, intereses, preferencias de consumo e incluso probabilidades de decisiones futuras.

Este proceso configura lo que aquí denominamos el perfil invisible: una identidad inferida que no siempre coincide con la autoimagen del usuario, pero que guía la personalización de contenidos, la priorización de información y la orientación de mensajes comerciales.

¿Qué es una huella digital?

Una huella digital es el conjunto de datos y rastros que una persona deja al interactuar con servicios digitales. Puede generarse de manera activa (por ejemplo, al publicar contenido) o pasiva (por ejemplo, mediante sistemas de seguimiento), y suele utilizarse para identificar, clasificar o inferir características del usuario.

- Historial de navegación
- Ubicación geográfica
- Compras online
- Interacciones sociales
- Información demográfica
- Preferencias de consumo

Cómo las empresas construyen tu identidad digital

La construcción de la identidad digital por parte de las empresas suele seguir un flujo de captura, análisis, integración y activación de datos, con el objetivo de convertir señales cotidianas en decisiones automatizadas de segmentación y personalización.

Recopilación de datos de navegación

Los sistemas de seguimiento como cookies, píxeles y técnicas de fingerprinting registran páginas visitadas, tiempos de permanencia, clics y rutas de navegación. Estos datos permiten inferir intereses inmediatos y construir historiales que, al persistir en el tiempo, describen rutinas informativas y preferencias de consumo.

Análisis mediante Inteligencia Artificial

Mediante modelos de aprendizaje automático, las empresas identifican patrones de comportamiento, agrupan usuarios en segmentos y estiman probabilidades (por ejemplo, propensión a compra o abandono). La IA no solo clasifica, sino que también predice: a partir de correlaciones, puede anticipar necesidades, estados de ánimo o intereses emergentes con fines de optimización comercial.

Integración de múltiples plataformas

La identidad digital se refuerza cuando se combinan datos procedentes de redes sociales, aplicaciones móviles, servicios externos y bases de datos de terceros.

La vinculación entre dispositivos y cuentas facilita una visión unificada del usuario, reduciendo la fragmentación de señales y aumentando la precisión del perfil inferido.

Publicidad personalizada

Una vez construido el perfil, se activa en sistemas de publicidad programática para mostrar anuncios dirigidos según intereses, contexto y probabilidad de conversión. Esta personalización puede mejorar la relevancia percibida, pero también incrementa la capacidad de influir en la atención y en la toma de decisiones, especialmente cuando el usuario desconoce los criterios de segmentación.

Datos recopilados y posibles usos

Dato recopilado	Posible uso
Ubicación	Publicidad local
Historial web	Recomendaciones
Compras online	Predicción de consumo
Redes sociales	Predicción de consumo
Dispositivo utilizado	Segmentación comercial

Implicaciones Éticas

La recopilación masiva de datos plantea desafíos directos para la privacidad: la información se obtiene a menudo mediante interfaces complejas, políticas extensas y mecanismos de consentimiento que no garantizan comprensión real. La falta de transparencia sobre qué se recoge, cómo se combina y con quién se comparte dificulta el control individual y amplía la asimetría entre usuarios y plataformas.

Además, la lógica de la personalización puede derivar en vigilancia digital y en formas sutiles de manipulación de decisiones, al priorizar contenidos y anuncios que maximizan objetivos comerciales.

Surge así una cuestión ética central: ¿cuáles deben ser los límites del acceso y uso de datos personales, y cómo equilibrar la innovación tecnológica con la protección de derechos fundamentales como la autonomía, la no discriminación y la intimidad?

Conclusiones

La identidad digital se ha convertido en un recurso de alto valor: a partir de la recolección continua de datos, las empresas pueden construir perfiles detallados que describen y predicen comportamientos. Este “perfil invisible” opera como una capa interpretativa que condiciona qué información vemos, qué ofertas recibimos y cómo se nos clasifica dentro de sistemas automatizados.

Comprender cómo se generan estos perfiles es un paso clave para un uso más consciente de la tecnología y para la adopción de prácticas responsables de privacidad. En el ámbito universitario y social, la educación digital y la exigencia de transparencia junto con marcos regulatorios efectivos resultan esenciales para promover un ecosistema que aproveche la innovación sin comprometer la protección de derechos fundamentales.

DAVID LANCHEROS IPUS

EL DISFRAZ DE LA PUBLICIDAD

¿Cuántas decisiones están tomadas por ti y cuántas de esas decisiones las toma alguien que te conoce pero tú no? Muchas veces la publicidad es personalizada sin darnos cuenta, algo simple detrás de lo cual se esconde algo mucho más complejo.

Cada búsqueda, cada clic y cada acción que tomemos en redes sociales alimenta una huella digital que vamos dejando poco a poco, huella de la cual las empresas se aprovechan y convierten en perfiles y patrones. Partiendo de este punto, los anuncios dejan de ser algo general y pasan a adaptarse a cada persona y a cada estilo con una precisión cada vez mayor. Pero ¿te has preguntado que esta supuesta comodidad también puede convertirse en una forma de influencia silenciosa a gran escala, difícil de detectar y aún más difícil de evitar?

De rastro digital a perfil de consumo

La lógica de la publicidad viene de una idea simple: cuanto más sabe una empresa sobre una persona, más fácil le resulta venderle algo. Por ello, plataformas y marcas analizan hábitos de navegación, compras previas, tiempo de visualización, ubicación y preferencias de consumo. ¿Te ha pasado que piensas en algo que quieres comprar, comer o visitar y, justo después, empiezan a aparecer anuncios de eso mismo? La verdad es que todos esos perfiles de consumo permiten clasificar al usuario por intereses, edad, nivel adquisitivo o probabilidad de compra. Así, la publicidad ya no se dirige a un público amplio, sino a sectores concretos que reciben mensajes diseñados para ellos.

La materia prima de las grandes empresas

El rastro que dejamos se ha convertido en el recurso principal de las grandes empresas. No se trata solo de lo que una persona publica de forma consciente, sino también

de lo que deja al moverse por internet: páginas visitadas, productos consultados, pausas en un vídeo o clics repetidos sobre un mismo contenido, condiciones aceptadas... Cada acción se interpreta como una pista para las grandes empresas. Esa acumulación de información les permite construir una imagen muy detallada del consumidor al cual dirigirse, aunque este no sea plenamente consciente de ello.

Casos concretos de influencia

Uno de los ejemplos más claros es Amazon. La plataforma más conocida de compra online en la actualidad no solo te muestra productos, sino que aprende de lo que cada usuario mira, compra o abandona en el carrito para sugerir nuevos artículos.

Ese sistema de recomendaciones puede ser útil, pero también empuja a comprar más de lo previsto. El usuario cree encontrar mejores opciones por su cuenta, cuando en realidad un algoritmo está priorizando aquello que considera más probable que le haga gastar.

La recomendación constante

Amazon representa bien el funcionamiento de la personalización con el usuario. Si una persona consulta un libro, unos auriculares o un juguete, el sistema empieza a mostrar productos relacionados durante días. Esa insistencia no es una simple casualidad: la lógica y la intención es mantener la atención y aumentar la probabilidad de terminar una compra.

La recomendación deja de ser un simple servicio y se convierte en una estrategia para orientar decisiones de compra de forma continua.

Instagram, TikTok y la publicidad camuflada

Las redes sociales llevan esta idea un paso más allá. En plataformas como Instagram o TikTok, la publicidad se integra dentro del propio contenido, de modo que el usuario la consume constantemente en segundo plano, y por eso no siempre percibe cuándo está viendo un anuncio y cuándo no. Esta táctica hace que el entretenimiento y la promoción sean cada vez más persuasivos.

Cuando un vídeo patrocinado aparece mezclado con publicaciones normales, el impacto comercial resulta más potente porque la atención del usuario ya está capturada.

Cuando el dato se convierte en presión

El gran problema de este modelo no es solo observar al consumidor, sino incitarlo a actuar de una determinada manera. Por ejemplo, pagar para consumir menos publicidad, repetir un anuncio varias veces, mostrar una oferta justo después de una búsqueda o insistir en productos similares a los que alguien ya consultó crea esa sensación de necesidad.

La decisión parece libre, pero muchas veces ha sido guiada por un sistema que nos conoce demasiado bien.

En ese punto, la personalización deja de ser una mejora y empieza a parecer una forma de presión constante e intrusiva sobre nuestra privacidad.

La polémica del consentimiento

Otro punto crítico es el del consentimiento. En teoría, el usuario acepta el tratamiento de sus datos, pero en la práctica muchas veces lo hace sin leer las típicas condiciones extensas, con formularios poco claros y sin entender realmente el alcance de lo que autoriza y está aceptando. Ahí nace una polémica importante:

¿podemos hablar del consentimiento libre cuando la mayoría de personas acepta de manera automática y obligatoria para seguir usando un servicio? La respuesta no es sencilla, pero sí revela que la relación entre empresas y consumidores está lejos de ser equilibrada.

¿Gratis o pagado con datos?

Has escuchado aquel dicho: "Cuando las cosas son gratis, el producto eres tú". Muchas plataformas se presentan como gratuitas, aunque el pago real esté en la cesión de tu información personal. Esa aparente gratuidad es parte del disfraz.

Recibimos acceso a una red social, una aplicación o una tienda online, pero cambio entregamos datos que luego se utilizan para perfilar nos y monetizar nuestro comportamiento. En ese intercambio, la sensación de no pagar dinero oculta un coste mucho menos visible: la pérdida de control sobre la propia información.

Un negocio basado en la atención

La publicidad personalizada no solo nos vende productos, también venden atención. Cuanto más tiempo permanece una persona dentro de una plataforma, más datos genera y más rentable se vuelve. Por eso el sistema está diseñado para captar la atención, prolongar la conexión y reforzar hábitos de consumo, incluso de adicción. Las empresas no buscan únicamente que el anuncio sea visto, sino que resulte lo bastante persuasivo o entretenido como para transformar la exposición en compra.

En ese proceso, el consumidor se convierte en el centro del negocio sin tener siempre la sensación de estar siendo observado.

Tiendas online y seguimiento constante

La intrusión de la privacidad es tan constante que un ejemplo muy claro es el de las tiendas online que “persiguen” al usuario con anuncios del producto que acaba de mirar. Esa repetición puede parecer una casualidad, pero en realidad responde al seguimiento de la actividad digital entre diferentes plataformas.

El objetivo es simple: recordar, insistir y convertirse. Lo que comienza como una visita informal termina muchas veces en una compra impulsiva, impulsada por la insistencia y la capacidad de las marcas para aparecer en el momento exacto.

Conciencia de lo que aceptamos

La publicidad personalizada se ha convertido en un sistema elegante que observa, clasifica y orienta al consumidor con una precisión cada vez mayor. Su disfraz consiste en presentarse ante ti de forma casi intuitiva y transparente, cercana y cómoda, cuando en realidad también funciona como un mecanismo de influencia comercial. Casos como Amazon, Instagram y TikTok muestran que el uso de datos no es neutro: puede condicionar decisiones, reforzar impulsos y reducir la capacidad de elegir con libertad.

Por eso, hablar de publicidad personalizada es también hablar de poder, de control y de la necesidad de mirar con más atención lo que aceptamos cada día. Debemos tomar conciencia de lo que aceptamos y decidir si estamos dispuestos a contribuir a este monopolio o a ser el producto.

GABRIEL FALCAO SANTOS

CURRICULUM SHADOW

Durante décadas, el currículum vitae tradicional ha operado como el documento de identidad profesional por excelencia. Un texto meticulosamente redactado, diseñado para destacar los éxitos, maquillar las brechas temporales y proyectar una versión idílica del candidato. Sin embargo, en el ecosistema corporativo actual, las grandes multinacionales han dejado de confiar ciegamente en lo que el candidato escribe sobre sí mismo. Hoy en día, las corporaciones buscan el "CV Shadow" (o Perfil Sombra).

El CV Shadow no es otra cosa que el dossier invisible pero imborrable construido a partir de la huella digital del postulante. Desde comentarios antiguos en foros públicos, interacciones en plataformas de ocio, fotografías etiquetadas por terceros, hasta el historial de publicaciones en redes sociales personales. Toda esta actividad fragmentaria es rastreada, consolidada e interpretada por herramientas avanzadas de adquisición de talento mucho antes de que el postulante sea convocado a una entrevista formal.

La Opacidad del Reclutamiento Algorítmico

Las grandes corporaciones se enfrentan a un volumen ingente de solicitudes para cada vacante. Para procesar esta avalancha de datos, los departamentos de Recursos Humanos han integrado sistemas automatizados conocidos como ATS (Applicant Tracking Systems) enriquecidos con algoritmos de Inteligencia Artificial y metodologías de OSINT (Inteligencia de Fuentes Abiertas).

Estas herramientas no solo verifican la experiencia técnica descrita en el PDF del candidato; ejecutan un escaneo periférico de la identidad digital pública del individuo. Analizan patrones de lenguaje, afinidades expresadas implícitamente y variables conductuales. El problema crítico reside en la opacidad del proceso: el candidato es comúnmente descartado por un algoritmo de evaluación de riesgos reputacionales sin llegar a saber jamás qué comentario de su adolescencia o qué interacción digital activó la alerta en el sistema.

El Concepto de Negocio "CV Shadow Suite"

Frente a este escenario de asimetría de información nace la oportunidad de una infraestructura tecnológica disruptiva: una plataforma que democratice el acceso a la propia información reputacional del candidato.

Concebida como un "Buró de Crédito para la Reputación Laboral", esta solución opera en dos vertientes altamente complementarias y éticas:

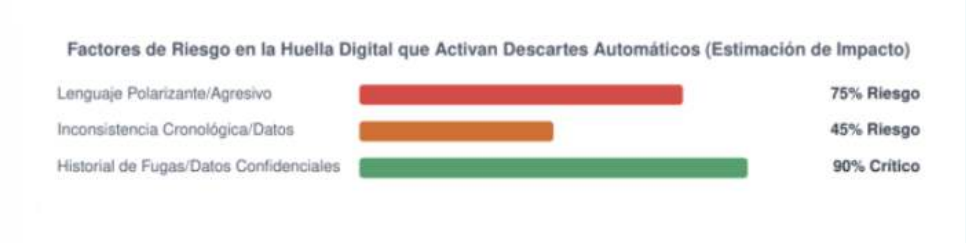
Para el Candidato: El Abogado Digital

A través de un motor de IA que emula de forma precisa los algoritmos de filtrado corporativo de las multinacionales de la lista Fortune 500, la plataforma permite al usuario mapear su estatus de contratación antes de postularse. El sistema ofrece un escaneo profundo en tres niveles: la web superficial (redes indexadas), foros comunitarios y bases de datos públicas de filtraciones (donde el usuario podría figurar como víctima de hackeo sin saberlo).

Tras el análisis, la plataforma provee un Score de Contratabilidad y herramientas automatizadas para la purga y el archivo de contenido de riesgo, aplicando mecanismos automatizados basados en el marco legal del Derecho al Olvido.

Equilibrio Corporativo: Contratación Ética y Cumplimiento

Para las grandes corporaciones, el espionaje digital informal de candidatos plantea serios dilemas legales respecto a la privacidad (como el cumplimiento estricto del RGPD europeo o legislaciones locales de protección de datos). Las empresas necesitan conocer el nivel de riesgo de un perfil sin incurrir en sesgos discriminatorios de género, raza, ideología u orientación.



La solución de plataforma propone un modelo de Certificación Blindada. El software evalúa al candidato con su consentimiento expreso, procesa el mapa completo de riesgos y emite un veredicto de cumplimiento exclusivamente vinculado a variables laborales válidas (ej. prevención de acoso digital o protección de secretos comerciales), anonimizando el resto de los datos sensibles que podrían viciar el proceso de selección.

Conclusión

El paradigma laboral ha cambiado permanentemente. El talento ya no se evalúa en un espacio aislado de dos páginas en blanco y negro; se juzga en el vasto e hiperconectado archivo de la red. Herramientas de la categoría de CV Shadow no buscan falsear la identidad del candidato, sino devolverle la gobernanza sobre sus propios datos en un mercado automatizado que, de lo contrario, amenaza con juzgar el futuro profesional a través de los ecos no contextualizados del pasado digital.

Arquitectura de monetización y sostenibilidad financiera

Segmento	Modelo de Negocio	Propuesta de Valor Clave
B2C (Candidatos premium)	Suscripción mensual recurrente durante la fase de búsqueda activa de empleo	Acceso a simulador de ATS, alertas de menciones en tiempo real y borrado automatizado por API
B2B (Grandes empresas)	Licenciamiento SaaS basado en el volumen anual de vacantes y candidatos evaluados	Mitigación del riesgo reputacional interno, blindaje legal contra demandas por sesgos y optimización del tiempo de selección

HUGO HERNÁNDEZ MORENO

Browser fingerprinting:

CÓMO TE IDENTIFICAN SIN QUE LO SEPAS

Imagina entrar a una tienda con la cara tapada, guantes puestos y sin decir tu nombre. Aun así, el dependiente te reconoce. Sabe que estuviste ayer, qué miraste, cuanto tiempo te quedaste frente a cada estante, e incluso que cojeas ligeramente de la pierna derecha. No te ha visto la cara. Pero te conoce mejor que tú a él. Eso, exactamente, es lo que ocurre cada vez que abres un navegador.

Durante años, las cookies fueron el mecanismo principal de rastreo online. Pequeños archivos que los sitios web depositaban en tu dispositivo para recordarte en la siguiente visita, como si el comercio te dejara una marca en el abrigo al salir.

La respuesta de los usuarios fue borrarlas. La respuesta de la industria fue inventar algo mejor, algo que no puedes borrar porque nunca estuvo guardado en tu dispositivo: el browser fingerprinting, o huella digital de navegador.

Sin cookies, sin login, sin escapatoria

El fingerprinting no almacena nada en tu dispositivo. En cambio, lee lo que ya está ahí. Cada vez que visitas una página web, tu navegador comparte, de forma completamente silenciosa, una cantidad sorprendente de información técnica: qué sistema operativo usas, qué fuentes tienes instaladas, la resolución y profundidad de color de tu pantalla, los plugins activos, el idioma configurado, la zona horaria, la velocidad de tu conexión e incluso cómo tu tarjeta gráfica renderiza ciertos elementos visuales.

Piénsalo como una sala llena de personas. Nadie lleva identificación. Pero si miras con atención, puedes distinguirlas por la altura, el color del pelo, el modelo de zapatillas, el acento al hablar, la forma de cruzar los brazos. Ningún detalle solo basta. Todos juntos, son irrepetibles.

Eso es exactamente lo que hace el fingerprinting con tu navegador.

Estudios de la EFF (Electronic Frontier Foundation) han demostrado que más del 80% de los navegadores pueden identificarse de forma unívoca solo a partir de estas características técnicas, sin necesidad de ningún dato personal declarado.

Las técnicas más sofisticadas van más allá de lo que el navegador declara voluntariamente. El canvas fingerprinting le pide a tu navegador que dibuje una imagen invisible en segundo plano y luego lee el resultado. Dado que cada combinación de hardware, sistema operativo y drivers gráficos produce mínimas variaciones en ese dibujo, el resultado actúa como una firma. El AudioContext fingerprinting hace lo mismo pero con sonido: genera una onda de audio que nunca llegas a escuchar, y mide cómo tu sistema la procesa internamente.

Son como pruebas de caligrafía que nunca pediste hacer, y que alguien guarda en un archivo con tu nombre.

¿Quién lo usa y para qué?

Las grandes plataformas tecnológicas, redes de publicidad y empresas de análisis de datos utilizan estas técnicas de forma rutinaria.

El objetivo es construir perfiles de comportamiento persistentes: qué contenido consumes, cuánto tiempo dedicas a cada tema, a qué hora del día navegas, qué tipo de noticias te hacen quedarte más tiempo en la página, desde qué dispositivos te conectas y en qué orden.

Ese perfil no se usa solo para mostrarte anuncios. Se usa para personalizar los precios que ves, el orden en que aparecen los resultados de búsqueda, qué noticias se priorizan en tu feed y qué productos aparecen destacados. La experiencia que percibes como neutra, como simplemente "internet", está siendo adaptada en tiempo real a lo que el algoritmo sabe de ti. No estás viendo la web.

Estás viendo tu versión de la web, esculpida a partir de tu comportamiento.

Hay algo más inquietante todavía: estos perfiles se comparten y se venden. Una empresa que nunca has visitado puede saber que eres del tipo de persona que compra impulsivamente por las noches, que lee sobre ansiedad los domingos o que ha buscado información sobre cambiar de trabajo tres veces este mes. No porque te haya espiado directamente, sino porque alguien que sí lo hizo le vendió esa información.

El negocio es enorme. El mercado global de datos de comportamiento de usuarios superó los 250.000 millones de dólares en 2023, y el fingerprinting es una pieza clave de esa cadena de valor.

El problema del consentimiento

Lo más relevante no es que la tecnología exista, sino que opera completamente fuera del marco de consentimiento que la mayoría de usuarios entiende. Cuando aceptas las cookies de un sitio web, crees haber tomado una decisión informada. Sientes que tienes el control. Pero el fingerprinting no requiere cookies, no requiere tu aceptación y, en muchos casos, ni siquiera aparece mencionado en la política de privacidad. Es el rastreo que ocurre después de que cree haber dicho que no.

Es como si en ese contrato que firmas sin leer hubiera una cláusula en letra minúscula que dijera: "Además, y con independencia de lo anterior, te observaremos siempre".

El RGPD europeo establece que cualquier tratamiento de datos que pueda usarse para identificar a una persona requiere base legal y, en muchos casos, consentimiento explícito. La huella de navegador, al poder vincularse con un individuo concreto, entra claramente en esa categoría. Sin embargo, la aplicación real es inconsistente. La asimetría técnica entre las empresas que rastrean y los reguladores que deberían supervisarlas hace que la fiscalización sea enormemente difícil. No es que la ley no exista. Es que los mecanismos para hacerla cumplir van varios años por detrás de la tecnología que pretende regular.

¿Qué puedes hacer?

Las opciones son limitadas, pero existen. Navegadores como Firefox o Brave incluyen protecciones activas contra fingerprinting, introduciendo ruido en los datos que comparten para que la huella sea menos precisa. El modo incógnito, contrariamente a la creencia popular, no protege contra esto en absoluto: oculta tu historial local, pero no cambia cómo tu navegador se identifica ante el mundo.

Las VPNs tampoco resuelven el problema, ya que el fingerprinting opera a nivel de navegador, no de red.

La solución más efectiva es también la más irónica: parecer lo más común posible. Cuanto más estandarizado sea tu entorno, menos única es tu huella. Usar el navegador por defecto, sin extensiones, con la configuración estándar, te hace invisible precisamente porque eres indistinguible de millones de personas. En un ecosistema diseñado para diferenciarte y clasificarte, la mejor privacidad es la invisibilidad por mediocridad.

Aunque claro, hay algo profundamente contradictorio en tener que volverse genérico para proteger la propia individualidad.

Lo que no puedes no saber

Cada vez que navegas, dejas una firma. No en el sentido metafórico de "dejas rastro", sino en el sentido técnico y literal: una combinación de señales que los sistemas de las grandes plataformas pueden asociar a ti con una precisión que supera a la de muchos documentos de identidad.

No hace falta que hayas iniciado sesión en ningún sitio. No hace falta que hayas aceptado nada. No hace falta que hayas hecho nada malo. Solo hace falta que hayas abierto el navegador.

La pregunta que vale la pena hacerse no es si esto debería preocuparte. La pregunta es qué tipo de internet queremos construir: uno donde la identificación constante y silenciosa sea el precio por defecto de participar, o uno donde la privacidad no sea un privilegio técnico reservado a quien sabe cómo protegerse, sino un derecho que funciona para todo el mundo.

"La huella digital no es una metáfora. Es un mecanismo técnico real, silencioso y casi imposible de evitar. Entenderlo es el primer paso para no ser solo un punto de datos en la hoja de cálculo de otra empresa."

IGNACIO QUIROZ COSCOLLANO

THE DATA MONOPOLY OF BIG TECH

When the digital world belongs to a few companies

The internet was once imagined as a decentralized space, a network where information could flow freely between individuals, institutions, and communities. It promised openness, innovation and equal access to knowledge. Today, however, much of that digital ecosystem is concentrated in the hands of a small number of corporations.

Every search query, online purchase, social interaction, and cloud-stored document passes through infrastructures owned by a handful of technology companies. Platforms such as Google, Meta, Amazon, Microsoft, and Apple have become more than service providers; they have evolved into the foundations upon which digital life operates.

This concentration is not limited to market power. These companies control the data generated by billions of users while simultaneously owning the systems used to collect, store, process, and analyze that information. Data centers, cloud infrastructures, artificial intelligence models, advertising networks, and social platforms are increasingly interconnected under the control of the same actors.

As a result, participation in the digital world often requires interacting with infrastructures that are neither public nor neutral. Every digital activity leaves traces, and those traces become valuable assets. Information has become one of the most important resources of the twenty-first century, and the organizations that control it occupy a position of unprecedented influence. This raises a fundamental question: if a small group of companies controls both the data and the mechanisms required to exploit it, who ultimately controls the digital environment itself?

The answer is not only an economic concern. It is also a cybersecurity issue.

The digital footprint as a resource

Every interaction performed online generates data. Some of this information is provided consciously, such as names, email addresses, or photographs. Much of it, however, is collected indirectly through browsing behavior, device characteristics, location data, purchase history, and patterns of interaction.

Individually, these pieces of information may appear insignificant. Combined, they create detailed digital profiles capable of revealing habits, preferences, routines and even predictions about future behavior. The digital footprint has become a resource that can be analyzed, categorized, and monetized at a massive scale.

Artificial intelligence has accelerated this process. Modern machine learning systems can process enormous volumes of user data and identify patterns that would be impossible for humans to detect manually. Through continuous analysis, algorithms can estimate interests, purchasing intentions, political preferences and behavioral tendencies with remarkable accuracy.

From a business perspective, this capability enables highly personalized services and targeted advertising. However, it also increases the concentration of informational power. The more data a company possesses, the more effectively its algorithms operate. In turn, better algorithms attract more users, generating even more data.

This creates a self-reinforcing cycle that strengthens the position of dominant platforms.

The consequence is that data is no longer simply a byproduct of digital activity. It has become the fuel that powers the modern internet. Those who control the largest data ecosystems gain advantages that are increasingly difficult for competitors to challenge.

Security at scale: when a breach affects millions

The concentration of information creates efficiency, but it also creates risk.

Because major technology companies store data belonging to billions of individuals, they represent highly attractive targets for cybercriminals.

A successful attack against a single platform can expose information on a scale rarely seen in other sectors.

History provides numerous examples of this vulnerability. Large-scale data breaches affecting social networks, cloud providers and online services have exposed personal information, login credentials and sensitive user records. While the specific causes vary, the underlying reality remains the same: when vast amounts of information are concentrated in one place, the consequences of a security failure become exponentially greater.

Unlike traditional physical assets, digital information can be copied, distributed, and exploited almost instantly. Once data is leaked, recovering control becomes nearly impossible. Stolen information can be used for identity theft, financial fraud, credential stuffing attacks, or highly targeted social engineering campaigns.

This transforms cybersecurity into a systemic challenge. The security of an individual user increasingly depends on the security practices of organizations that store their information.

Even users who follow strong security habits may be affected by breaches occurring far beyond their direct control.

The larger the repository of data, the greater the responsibility attached to its protection. Yet the same scale that makes these platforms powerful also makes them attractive targets.

Surveillance, algorithms and digital influence

The debate surrounding Big Tech extends beyond data breaches. Security concerns are also linked to the ability to observe and influence user behavior.

Digital platforms continuously collect information in order to optimize services, improve recommendations, and personalize content.

In practice, this means that algorithms determine much of what users see, read, and interact with online. News feeds, search results, advertisements, and recommendations are increasingly curated through automated systems.

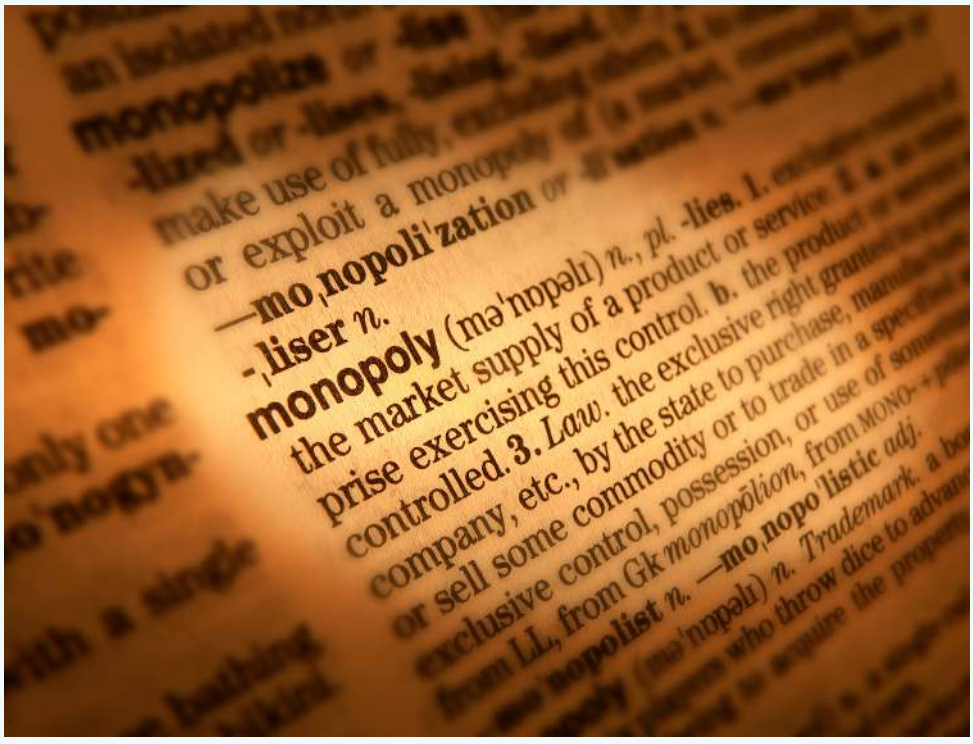
These mechanisms are not inherently malicious. They are designed to improve efficiency and relevance. However, their influence raises important questions regarding transparency and accountability. .

When algorithms shape access to information, they indirectly shape decision-making processes. The data collected from users becomes the foundation for systems capable of predicting and influencing behavior. In this context, surveillance is not necessarily the result of a single actor observing individuals directly. Instead, it emerges through continuous data collection and automated analysis performed at scale.

From a cybersecurity perspective, this concentration of information creates additional risks.

The more detailed user profiles become, the more valuable they are to malicious actors. Data intended for personalization can also be exploited for phishing campaigns, impersonation attempts, and sophisticated social engineering attacks.

The same information that enables convenience can also increase exposure.



Dependency on private digital infrastructures

Perhaps the most significant aspect of the Big Tech ecosystem is not the data itself, but the infrastructure that supports it.

A large portion of the internet relies on cloud services operated by a small number of providers. Businesses, governments, educational institutions and critical services increasingly depend on privately owned infrastructures to store information and deliver digital services.

This concentration introduces a new form of dependency. If a major cloud provider experiences a disruption, the effects can cascade across thousands of organizations simultaneously. What appears to be a technical failure in one company can quickly become a broader societal problem.

The issue is not simply operational reliability. It also concerns governance, control, and resilience.

As digital infrastructures become essential to everyday life, questions emerge regarding who owns them, who regulates them, and how they should be protected.

Cybersecurity is therefore no longer limited to protecting individual devices or networks. It increasingly involves safeguarding the underlying infrastructures upon which entire digital ecosystems depend.

Data protection in an age of concentration

The growing power of Big Tech has prompted regulatory responses aimed at protecting users and limiting potential abuses. In Europe, the General Data Protection Regulation (GDPR) established new standards regarding consent, transparency, and data-handling practices.

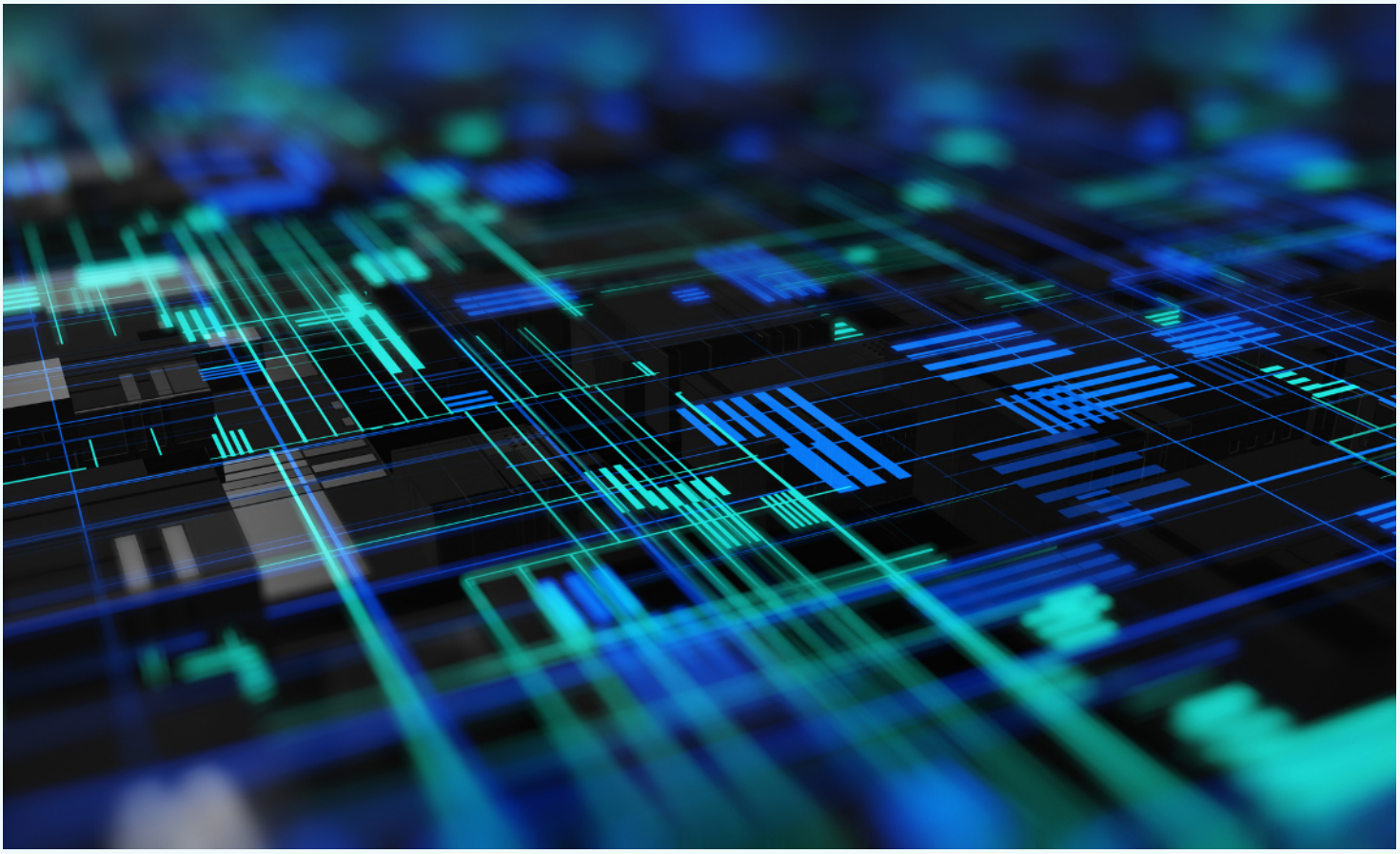
These measures represent an important step toward balancing innovation with privacy rights. Nevertheless, regulation alone cannot eliminate the structural reality of data concentration.

The volume of information collected continues to expand, and technological capabilities continue to evolve.

The challenge facing modern societies is therefore not only how to secure data but also how to govern systems that derive power from accumulating it. Security, privacy, and transparency are increasingly interconnected concerns.

The digital economy depends on data, but democratic societies depend on trust. Maintaining that trust requires more than technological innovation; it requires accountability, oversight and a continuous commitment to protecting the individuals whose information fuels the digital world.

Because in the era of Big Tech, the question is no longer whether our data has value. The question is who controls that value, and what happens when so much of it belongs to so few.



JORGE MADRID VALNICKAS

La ilusión de la privacidad en la era hiperconectada

En la actualidad, el concepto tradicional de privacidad se ha desvanecido frente al avance implacable de la digitalización global. Cada interacción que realizamos en internet, desde aceptar cookies hasta utilizar aplicaciones móviles aparentemente inofensivas, contribuye a desmantelar nuestro anonimato. La sociedad asume erróneamente que navegar en modo incógnito o utilizar pseudónimos garantiza la confidencialidad, ignorando que la infraestructura de la red está diseñada para registrar cada acción. Esta falsa sensación de seguridad es el terreno fértil donde opera el complejo mercado de datos, un ecosistema donde nuestra identidad digital se expone y comercializa sin nuestro consentimiento real.

El rastro invisible de nuestra huella digital

Constantemente generamos un flujo inmenso de metadatos que documenta nuestra rutina diaria con una precisión alarmante. Estos registros silenciosos incluyen historiales de geolocalización, hábitos de consumo y patrones de búsqueda, conformando una huella digital prácticamente imborrable.

El fin del anonimato: QUIÉN COMPRA Y VENDE TU RASTRO EN INTERNET

> *"Hoy eres menos valioso que los datos que produces"*
> *- Watch Dogs*

Al carecer de barreras protectoras adecuadas, esta información permite a terceros reconstruir perfiles altamente detallados, demostrando que el anonimato online es hoy una utopía.

La transformación del usuario en la mercancía del siglo XXI

El modelo económico de internet ha evolucionado para centrarse en la extracción y análisis sistemático de información personal. Las plataformas que utilizamos gratuitamente no son altruistas; su verdadera rentabilidad radica en convertir al usuario en el producto. Así, la privacidad comercializada se vuelve la norma establecida, donde cada interacción alimenta el voraz capitalismo de vigilancia que domina el ciberespacio actual.

El modelo de negocio opaco de los data brokers

Detrás de la recolección de información existe un entramado corporativo altamente lucrativo y sumamente oscuro. Los intermediarios de datos operan en las sombras, actuando como entidades que no interactúan directamente con el usuario, pero que acumulan y procesan vastas cantidades de información personal. Este modelo de negocio se nutre de la ignorancia generalizada sobre los términos de servicio que aceptamos ciegamente a diario.

Su rentabilidad se basa en ensamblar fragmentos de actividad aislada para construir un perfilamiento exhaustivo del individuo. Posteriormente, este mercado gris vende estas identidades digitales al mejor postor sin que exista una supervisión real o consentimiento explícito.

Recopilación masiva: cómo extraen y cruzan nuestra información

Las aplicaciones modernas funcionan como aspiradoras de contexto. Plataformas sociales como BeReal, bajo la premisa de la espontaneidad, operan capturando el entorno sin filtros del usuario. A través de sus imágenes duales, documentan rutinas precisas, analizando las calles que transitas, tus aficiones y el diseño de tu hogar. Esta extracción silenciosa transforma tu vida diaria y tus patrones de comportamiento en coordenadas geográficas y datos perfectamente estructurados.

El mercado en la sombra: quién compra nuestros perfiles y para qué

Una vez empaquetada, esta información íntima se subasta a múltiples actores. Los compradores abarcan desde corporaciones de marketing hiperdirigido hasta entidades financieras o aseguradoras que evalúan riesgos basándose en tu comportamiento rutinario.

En este comercio clandestino, la persona pierde por completo la soberanía sobre su identidad mercantilizada, desconociendo quién almacena sus datos, cuánto tiempo los retendrán o para qué decisiones algorítmicas están siendo utilizados.

Inteligencia de Fuentes Abiertas (OSINT): un arma de doble filo

La disciplina de la inteligencia de fuentes abiertas ha transformado radicalmente la forma en que se investiga en el ciberespacio. Originalmente concebida para la recolección de inteligencia militar y la prevención del fraude, esta metodología se basa en la búsqueda, recolección y análisis de datos disponibles públicamente en la red. Sin embargo, la democratización de estos conocimientos ha generado un escenario complejo y peligroso. La misma metodología que ayuda a los analistas a desarticular redes criminales está ahora al alcance de actores maliciosos. Este acceso indiscriminado facilita la recolección de información para orquestar ataques sofisticados, demostrando que el OSINT ofensivo representa una amenaza significativa para cualquier ciudadano conectado.

El uso legítimo en ciberseguridad vs. la explotación maliciosa

En manos de profesionales, estas técnicas sirven para evaluar la seguridad de la empresas mediante simulaciones de ciberataques. En contraste, los ciberdelincuentes explotan esta misma disciplina para realizar un reconocimiento exhaustivo de sus víctimas. De esta forma, construyen un perfil íntimo que facilita la manipulación y el fraude,desvirtuando por completo el propósito original de la inteligencia pública.

Herramientas y técnicas automatizadas que exponen tu vida

La existencia de programas especializados o buscadores avanzados ha simplificado enormemente la extracción de datos. Estas plataformas permiten cruzar información de foros, webs y redes sociales en cuestión de segundos.

Al emplear estas potentes herramientas automatizadas, cualquier atacante con conocimientos intermedios puede trazar un mapa detallado sobre el nivel de exposición y las vulnerabilidades de un individuo específico.

La tormenta perfecta: la convergencia de bases de datos y OSINT

Cuando la vasta información comercializada por los intermediarios de datos choca con las capacidades analíticas de la Inteligencia de fuentes abiertas, el resultado es devastador para la privacidad. Ya no se trata únicamente de información aislada o de rastros sueltos esparcidos por internet. La convergencia de ambos mundos permite cruzar inmensas bases de datos organizadas con información recopilada en tiempo real. Esta sinergia crea un ecosistema donde es posible predecir comportamientos futuros con una exactitud escalofriante, generando un escenario de vulnerabilidad extrema donde la fusión de datos expone nuestra intimidad ante atacantes y corporaciones.

Perfilado psicológico avanzado y microsegmentación predictiva

Al cruzar análisis OSINT con historiales masivos, las corporaciones logran un perfilado psicológico sumamente preciso. El ejemplo más claro es su capacidad de predecir qué producto exacto comprará un usuario antes incluso de que este formule la necesidad. Estos modelos matemáticos alimentan sistemas diseñados para ejercer una manipulación algorítmica que explota silenciosamente nuestras rutinas diarias.

Vectores de ataque: del spear phishing al robo de identidad

Toda esta exposición hiperdetallada facilita la creación de engaños personalizados que burlan nuestras defensas lógicas. Los cibercriminales utilizan este contexto para diseñar campañas de spear phishing casi imposibles de detectar, simulando urgencias reales o suplantando a familiares de confianza.

En los escenarios más graves, esta acumulación masiva de información personal desemboca en un robo de identidad total y catastrófico.

El marco regulatorio frente al vacío legal del mercado de datos

Ante la comercialización masiva de nuestra identidad, las instituciones han intentado establecer límites legales para proteger al ciudadano. Sin embargo, la velocidad de la innovación tecnológica y la opacidad de los intermediarios de información siempre van un paso por delante de la legislación vigente. Aunque existen normativas pioneras diseñadas para frenar los abusos corporativos, la realidad operativa demuestra que las leyes actuales presentan importantes vacíos jurisdiccionales. Esta discrepancia entre la teoría legal y la práctica técnica crea una inseguridad jurídica constante, permitiendo que el mercado gris de datos continúe expandiendo sus operaciones globales sin enfrentar consecuencias
reales y efectivas.

El impacto del RGPD (GDPR) y sus limitaciones prácticas

El Reglamento General de Protección de Datos supuso un hito en la defensa de la privacidad ciudadana.

No obstante, su efectividad real se diluye frente a estructuras corporativas internacionales complejas. La fatiga del consentimiento y los extensos términos legales convierten el cumplimiento en un mero trámite burocrático, limitando severamente la protección efectiva frente al rastreo indiscriminado.

La odisea técnica y burocrática del derecho al olvido

Solicitar la eliminación de nuestros rastros en internet resulta ser una batalla titánica y desgastante para cualquier individuo.

Los procedimientos exigen identificar cada entidad que posee nuestra información, un proceso casi imposible cuando los registros se revenden infinitamente. Además, la desindexación técnica rara vez garantiza un borrado definitivo en servidores ubicados en jurisdicciones o paraísos digitales remotos.

Recuperando el control: estrategias de mitigación y futuro

Llegados a este punto, la abrumadora realidad de la exposición online puede generar un profundo sentimiento de indefensión. Sin embargo, ceder al fatalismo no es la respuesta adecuada frente a estas amenazas.

Recuperar la soberanía sobre nuestra presencia en la red requiere un cambio de mentalidad radical, pasando de ser usuarios pasivos a individuos proactivos en la gestión de la información.

Aunque el anonimato absoluto sea inalcanzable en la arquitectura actual de internet, la implementación de hábitos de seguridad sostenibles ofrece una esperanza real. Reducir drásticamente nuestra huella digital es totalmente posible si comenzamos a aplicar una defensa activa.

Higiene digital y contramedidas de privacidad defensiva (OPSEC)

Aplicar principios de OPSEC (Seguridad Operativa), constituye nuestro primer escudo. Este concepto consiste en proteger pequeños detalles aparentemente inofensivos que, al unirse, revelan nuestros hábitos. Implica segmentar nuestra vida usando correos desechables, instalar bloqueadores de rastreadores y controlar la sobreexposición voluntaria.

Mantener esta higiene digital rigurosa entorpece en gran medida a los atacantes, encareciendo y complicando la recolección automatizada de nuestra información personal.

El paradigma emergente: hacia modelos de identidad descentralizada

El futuro de la privacidad exige dejar de regalar nuestra información a las grandes empresas tecnológicas. Los nuevos modelos proponen que cada persona custodie sus datos en su propio dispositivo.

Así, se podría demostrar un requisito, como ser mayor de edad, sin enseñar todo el documento. Esta gestión personal nos devuelve el control real y frena la
venta indiscriminada de nuestra vida.

La concienciación ciudadana como última línea de defensa

Para cerrar el círculo, debemos entender que la tecnología por sí sola no resolverá la vulnerabilidad a la que nos enfrentamos. El fin del anonimato no debe aceptarse como una condena inevitable, sino que debe servir como una llamada de atención urgente para toda la sociedad. Estudiantes, profesionales y ciudadanos deben comprender que su información íntima tiene un valor incalculable. Recuperar el terreno perdido frente al mercado opaco requiere educar y cuestionar constantemente qué entregamos a cambio de una falsa comodidad gratuita. Al final, la concienciación colectiva será el escudo más eficaz para evitar que nuestra identidad digital siga siendo una simple mercancía.

PABLO DEL RÍO MARTÍNEZ

LA HUELLA DIGITAL EN LA CONTRATACIÓN LABORAL

Hace no tantos años, prepararse para una entrevista de trabajo significaba planchar la camisa, repasar el currículum y ensayar mentalmente esa pregunta de ¿cuál es tu mayor defecto? intentando que la respuesta no sonara a confesión. Hoy, todo eso sigue siendo necesario, pero hay un paso previo que se nos suele olvidar: revisar lo que ya hemos publicado sobre nosotros mismos durante los últimos años en internet.

Porque, nos guste o no, cuando un reclutador recibe nuestro CV, lo primero que hace muchas veces no es leerlo. Es escribir nuestro nombre en Google.

Y ahí empieza la verdadera entrevista.

Tu CV ya no es solo tu CV

Durante décadas, el currículum fue una herramienta cuidadosamente diseñada: una página en la que cada uno se vendía a sí mismo en su mejor versión posible. Una especie de tráiler de película donde solo aparecían las mejores escenas. El problema es que hoy, el reclutador ya no se conforma con el tráiler. Quiere ver la película completa, los descartes, los bloopers y, si puede, también las críticas del público.

Según el último informe de InfoJobs sobre redes sociales y empleo, el 52% de las empresas en España consultan las redes sociales de los candidatos antes de tomar una decisión de contratación. A nivel internacional, las cifras son aún más llamativas: distintos estudios sitúan entre el 70% y el 94% el porcentaje de reclutadores que utilizan las redes sociales como parte habitual de su proceso de selección.

Es decir, mientras nosotros pensamos que LinkedIn es nuestro escaparate profesional y que Instagram o TikTok son nuestro espacio personal, para muchos reclutadores todo forma parte del mismo escaparate. La diferencia es que en uno hemos puesto los maniquíes con traje, y en el otro no nos hemos dado cuenta de que la persiana está subida.

La huella digital: ese tatuaje que no recordamos habernos hecho

La huella digital es, básicamente, todo el rastro que dejamos al usar internet. Publicaciones, comentarios, likes, fotos etiquetadas, opiniones en foros de hace una década, esa reseña enfadada que pusimos a un restaurante en 2017 porque la pizza llegó fría… todo cuenta. Y, a diferencia de los tatuajes, no hace falta ir a una sesión de láser para quitárnoslo: hace falta ir a las sesiones, y aun así, alguna foto siempre sobrevive.

Una buena forma de entenderlo es pensar en la huella digital como una caja negra de un avión. Registra todo lo que ha pasado: cada movimiento, cada turbulencia, cada decisión.

Cuando alguien quiere reconstruir quiénes somos, no necesita preguntárnoslo. Solo tiene que abrir la caja.

Y aquí está lo interesante: el 72% de los reclutadores considera que esos perfiles personales reflejan la realidad de un candidato mejor que un CV, según un estudio de Adecco. Es decir, confían más en lo que publicamos sin pensar que en lo que escribimos pensando mucho. Lo cual, si lo piensas, tiene bastante sentido. Pero da algo de vértigo.

¿Qué buscan exactamente cuando nos buscan?

No están comprobando si somos la persona más guay del mundo. Lo que un reclutador busca en nuestra huella digital se puede resumir en tres bloques:

- **Coherencia:** que lo que decimos en el CV cuadre con lo que se ve fuera. Si en el CV ponemos inglés nivel avanzado y nuestro último viaje a Londres lo contamos en Instagram como “adventur in london, very nais”, algo no cuadra.
- **Comportamiento y valores:** comentarios agresivos, insultos a antiguos jefes, opiniones extremas o fotos que comprometan la imagen profesional. Aquí no estamos hablando de censura, sino de cómo nos relacionamos con el mundo cuando creemos que nadie nos mira.
- **Marca personal:** si proyectamos algún tipo de coherencia profesional, interés por nuestro sector, capacidad de comunicar y de aportar valor.

Los datos son contundentes. Según la encuesta de CareerBuilder, el 57% de los reclutadores que investigan a candidatos en redes sociales ha encontrado contenido que les llevó a no contratarlos. Las razones principales: fotos inapropiadas, faltas de ortografía recurrentes, y rasgos de personalidad que no encajan con el puesto.

Sí, has leído bien: las faltas de ortografía. Resulta que escribir “haber” en lugar de “a ver” puede costar más caro que llegar tarde a una entrevista.

El nuevo entrevistador no parpadea: la IA llega a recursos humanos

Si pensábamos que ser revisados por un humano era ya bastante presión, la cosa se complica cuando entendemos quién está al otro lado del proceso. Cada vez más, no es una persona. Es un algoritmo.

Sistemas de inteligencia artificial analizan currículums, perfiles de LinkedIn, vídeos de entrevistas e incluso microexpresiones faciales para puntuar a los candidatos antes de que un humano los vea. Y aquí aparece un problema interesante: estos sistemas no son neutrales. Aprenden de datos pasados. Y los datos pasados, como todos sabemos, no siempre han sido modelo de equidad.

El caso más famoso es el de Amazon. En 2018, la compañía tuvo que descartar una herramienta interna de reclutamiento basada en IA porque, tras entrenarla con currículums recibidos durante una década en el sector tecnológico, el sistema aprendió algo bastante feo: penalizaba los CV que contenían la palabra “mujeres” (como en “club de ajedrez femenino”) y rebajaba la puntuación de las graduadas de universidades exclusivamente femeninas. El algoritmo no era machista por diseño; simplemente había aprendido a serlo observándonos a nosotros.

Es como esos niños que aprenden palabrotas no porque alguien se las enseñe formalmente, sino porque escuchan lo que oyen. La diferencia es que un niño se puede corregir con una conversación. Un modelo entrenado con sesgos hay que tirarlo entero y volver a empezar.

La caja negra del rechazo

Y aquí viene una de las partes más incómodas del asunto. Cuando una persona nos rechaza, al menos podemos pedir feedback.

Cuando un algoritmo nos rechaza, muchas veces ni siquiera sabemos que ha sido el algoritmo. Y desde luego, no sabemos por qué.

A este problema se le llama, en términos técnicos, “el problema de la caja negra”. Los modelos de IA modernos toman decisiones basadas en miles o millones de parámetros que ni siquiera sus creadores son capaces de explicar del todo. Te quedas fuera del proceso, pero no hay un "por qué" claro al que poder agarrarse. Solo un correo automático: “Hemos seguido adelante con otros candidatos”.

El Reglamento General de Protección de Datos europeo y la nueva Ley de IA intentan poner orden en este escenario, exigiendo transparencia, derecho a explicación y supervisión humana en las decisiones automatizadas que afecten significativamente a las personas. En la práctica, sin embargo, la regulación va siempre uno o dos pasos por detrás de la tecnología. Es la pescadilla de siempre: legislamos lo que ya está pasando mientras lo que viene ya está cambiando las reglas.

¿Significa esto que tenemos que borrar nuestras vidas de internet?

No exactamente. Borrar todo no solo es prácticamente imposible, sino que tampoco es necesariamente la mejor estrategia. Un perfil completamente vacío también levanta sospechas. Es como llegar a una entrevista sin DNI, sin teléfono y sin acordarse del nombre de la calle donde vives. Es raro.

La pregunta no es “¿cómo me oculto?”, sino “¿qué historia estoy contando sobre mí mismo en internet?” Porque, queramos o no, estamos contando una. La diferencia entre los candidatos que aprovechan su huella digital y los que la sufren no está en cuánto publican, sino en si han pensado lo que publican.

Algunas ideas prácticas, sin pretender ser exhaustivos:

• Búscate en Google a ti mismo cada cierto tiempo. Como un chequeo médico, pero digital. Sin reproches, solo por saber qué ven los demás.
• Revisa la privacidad de tus redes. No para esconder cosas malas, sino para decidir qué quieres que sea público y qué no.
• LinkedIn no es opcional. Si trabajas en un entorno profesional, tener un perfil cuidado en LinkedIn es hoy casi tan básico como tener email.
• Antes de publicar algo cuando estás enfadado, recuerda esta regla de oro: internet tiene memoria y los reclutadores tienen tiempo.
• No mientas en tu marca personal. La incoherencia entre lo que vendes y lo que se ve siempre acaba saliendo. Y se nota más de lo que pensamos.

El trasfondo: ¿quién decide quiénes somos?

Más allá de los consejos prácticos, hay una pregunta de fondo que conviene plantearse. Si cada vez son más las decisiones laborales, financieras, incluso afectivas, que se toman a partir de nuestra huella digital, ¿en qué momento dejamos de ser nosotros los que decidimos quiénes somos para que lo decida el rastro que dejamos?

Hasta hace no mucho, una persona podía cambiar de ciudad, de trabajo o de etapa vital y empezar de cero. Era literalmente posible reinventarse. Hoy, nuestra versión de hace diez años está a un par de clics de cualquier reclutador. Cada error que cometimos en la adolescencia, cada opinión desafortunada que escribimos los últimos años, cada foto que nos pareció graciosa entonces, sigue ahí, esperando. Esto plantea un dilema interesante. ¿Hasta qué punto es justo que un candidato sea juzgado, en 2026, por una publicación de 2014?

¿Y hasta qué punto es injusto que una empresa decida ignorar señales evidentes sobre cómo se comporta una persona cuando cree que nadie la observa?

Probablemente no haya una respuesta sencilla. Lo que sí parece claro es que estamos en un momento en el que la sociedad todavía no ha decidido del todo qué hacer con esta capacidad de recordarlo todo de todos. Y, como suele pasar con las tecnologías nuevas, mientras lo decidimos, la utilizamos.

Conclusión: ya no hay primera impresión, hay impresión continua

Aquella idea clásica de que “solo hay una oportunidad de causar una primera impresión” se ha quedado vieja. Hoy no hay una primera impresión. Hay una impresión continua, acumulada a lo largo de los años, generada con cada interacción digital, y disponible para cualquier persona o sistema que decida buscarnos.

La huella digital no es ni buena ni mala, igual que un martillo no es ni bueno ni malo. Depende de quién lo use y para qué. Lo verdaderamente importante es entender que ya forma parte de cómo el mundo nos evalúa, y que tenemos más control sobre ella del que solemos pensar.

Tal vez la próxima vez que vayamos a publicar algo, antes de pulsar el botón, podamos hacernos una pregunta muy simple: ¿estaría cómodo defendiendo esto delante de un futuro entrevistador que ni siquiera sé que existe todavía?

Si la respuesta es sí, adelante. Si la respuesta es “depende”, quizá merece la pena pensarlo unos segundos más.

Porque en un mundo donde nuestra huella digital habla por nosotros, lo mínimo que podemos hacer es asegurarnos de que cuenta la historia que realmente queremos contar.

PABLO GARCÍA OLLERO

La comodidad de lo invisible

Durante años hemos hablado de la huella digital como si fuera algo individual. Como si cada persona, al navegar por internet, fuera dejando pequeñas marcas propias: una búsqueda, una compra, una ubicación, un “me gusta”, una conversación, una foto, una preferencia musical o una duda escrita a medianoche en un buscador.

La idea parece sencilla: nosotros usamos la tecnología y, al usarla, dejamos un rastro. Pero esa explicación es demasiado cómoda. Nos permite pensar que la huella digital es solo una consecuencia accidental de nuestra vida conectada, una especie de polvo que se acumula detrás de nuestros pasos.

Sin embargo, la realidad es más profunda y más incómoda. Las grandes empresas no solo observan nuestra huella digital: la diseñan, la recogen, la interpretan y la convierten en valor económico. No esperan pasivamente a que dejemos rastros; construyen los caminos por los que caminamos, los botones que pulsamos, las recomendaciones que vemos y las opciones que creemos elegir libremente.

- La pregunta, entonces, no es solo: ¿qué datos dejamos en internet?

- La pregunta real es: ¿quién convierte esos datos en poder?

Porque la huella digital ya no es únicamente un asunto de privacidad individual. Es una infraestructura. Es una forma de mirar, clasificar y predecir el comportamiento humano.

Y, en manos de grandes empresas tecnológicas, se convierte en una nueva forma de poder corporativo: silenciosa, cotidiana y profundamente integrada en nuestra vida.

Huellas digitales y grandes empresas: EL RASTRO INVISIBLE DEL PODER CORPORATIVO

> *“Cada clic parece pequeño, pero juntos forman un mapa de nosotros que otros aprenden a leer mejor que nosotros mismos.”*

La huella digital no se deja: se extrae

Tendemos a imaginar la huella digital como una marca que dejamos detrás de nosotros. Pero quizá sea más preciso verla como una mina. Cada interacción cotidiana puede ser excavada, refinada y convertida en algo útil para una empresa.

Buscar una palabra en Google no es solo buscar una palabra. Ver un vídeo en TikTok no es solo ver un vídeo. Comprar en Amazon no es solo comprar. Usar Instagram no es solo mirar fotos. Cada acción genera señales: qué nos interesa, cuánto tiempo permanecemos, qué ignoramos, qué repetimos, qué nos detiene, qué nos irrita, qué nos seduce.

La diferencia entre el dato y la huella está en la interpretación. Un dato aislado puede parecer insignificante. Pero miles de datos combinados empiezan a formar un retrato. Y ese retrato no es necesariamente el que nosotros daríamos de nosotros mismos, sino el que resulta útil para predecirnos.

Aquí aparece el verdadero cambio: las grandes empresas ya no solo venden productos o servicios; muchas de ellas venden predicción. Predicen qué anuncio nos hará detenernos, qué vídeo nos mantendrá dentro de la aplicación, qué producto podríamos comprar, qué noticia nos hará reaccionar o qué contenido aumentará nuestro tiempo de uso.

¿Somos conscientes de ello? A veces sí. ¿Podemos evitarlo del todo? Probablemente no.

El problema no es simplemente que las empresas tengan datos. El problema es que la acumulación masiva de datos crea una asimetría: ellas saben cada vez más sobre nosotros, mientras nosotros sabemos muy poco sobre cómo nos clasifican.

Es como jugar una partida de ajedrez contra alguien que no solo ve el tablero, sino también nuestras partidas anteriores, nuestros impulsos, nuestros errores habituales y el tiempo exacto que tardamos en dudar antes de mover una pieza.

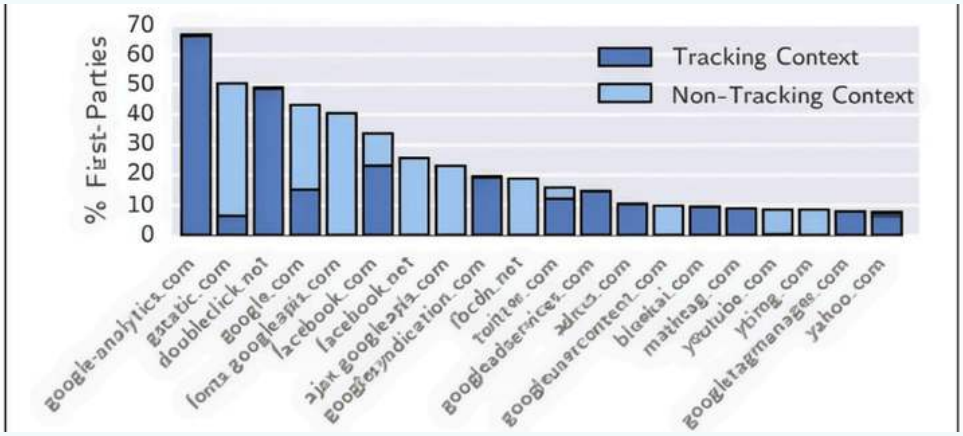


Imagen 1. Principales terceros presentes en la web y su papel en el rastreo digital.

La huella digital no se forma únicamente en la página que visitamos, sino también en la red de terceros que se activa detrás de cada visita. La figura muestra cómo determinados dominios y organizaciones aparecen de forma recurrente en sitios web, diferenciando contextos de tracking y no tracking.

Fuente: Englehardt, S. y Narayanan, A. (2016). Online Tracking: A 1-million-site Measurement and Analysis. Princeton University / ACM CCS.

El consentimiento como ritual vacío

En teoría, aceptamos. Pulsamos “aceptar cookies”, “continuar”, “permitir”, “he leído los términos y condiciones”. En la práctica, pocas veces entendemos realmente qué estamos aceptando.

El consentimiento digital se ha convertido en un gesto automático. Una puerta que atravesamos porque necesitamos llegar al contenido, a la compra, al servicio, a la aplicación. Nos piden permiso, sí, pero muchas veces dentro de un entorno diseñado para que aceptar sea lo más fácil y rechazar lo más incómodo.

Aquí entran los llamados patrones oscuros: diseños de interfaz que empujan al usuario hacia una decisión beneficiosa para la empresa. Botones más visibles para aceptar que para rechazar, procesos de cancelación largos, mensajes de urgencia, opciones escondidas o frases ambiguas que hacen parecer que decir “no” es perder algo importante. Por ende, una pregunta que deberíamos hacernos es: ¿Nos manipulan las interfaces digitales?

Lo cierto es que la respuesta es: Sí, en muchos casos.

La pregunta abierta de este tema sí es más difícil de plantear, ya que deberíamos preguntarnos lo siguiente: ¿cuántas de nuestras decisiones digitales siguen siendo realmente nuestras cuando el entorno está diseñado para conducirlas?

El caso de Amazon Prime, investigado por la FTC, es un ejemplo claro de este problema. La acusación no giraba simplemente en torno a una suscripción, sino en torno a una arquitectura de decisión: hacer fácil entrar y difícil salir. En ese punto, la tecnología deja de ser una herramienta neutral y se convierte en una especie de pasillo inclinado. Caminamos nosotros, pero el suelo ya estaba diseñado para empujarnos.

Los patrones oscuros muestran cómo ciertas decisiones digitales pueden ser guiadas por el diseño de la interfaz: temporizadores de urgencia, costes ocultos, suscripciones difíciles de cancelar, opciones preseleccionadas o mensajes diseñados para presionar al usuario.

Fuente: Mathur, A. et al. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proceedings of the ACM on Human-Computer Interaction.

Algoritmos: el espejo que también empuja

Hay una metáfora habitual para hablar de los algoritmos: son espejos. Nos muestran lo que nos gusta, lo que buscamos, lo que consumimos. Pero esta metáfora se queda corta. Un algoritmo no solo refleja; también empuja.

Si una plataforma detecta que ciertos contenidos nos retienen más tiempo, tenderá a ofrecernos más contenidos parecidos. Si detecta que reaccionamos ante la indignación, puede servirnos más indignación. Si aprende que una estética, una opinión o una emoción nos captura, puede convertir esa captura en rutina.

Esto no significa que los algoritmos controlen nuestra mente como una fuerza mágica. Sería exagerado y poco riguroso. Pero tampoco podemos fingir que son simples vitrinas neutrales. Los sistemas de recomendación ordenan la realidad digital. Deciden qué aparece primero, qué se repite, qué desaparece, qué se vuelve visible y qué queda sepultado.

La huella digital, en este sentido, no solo describe lo que somos. También participa en lo que acabamos viendo, pensando y deseando. Es un círculo: actuamos, el sistema aprende, el sistema nos muestra, nosotros reaccionamos y el sistema vuelve a aprender.

Por ello, nos salen distintas preguntas que debemos plantearnos:

- ¿Quién rompe ese círculo?
- ¿El usuario individual?
- ¿La empresa?
- ¿El regulador?
- ¿La sociedad?

La respuesta cómoda sería decir que cada persona debe aprender a usar mejor internet. Y sí, hay responsabilidad individual. Pero sería injusto cargar todo el peso sobre el usuario. Nadie puede “elegir libremente” dentro de un sistema cuyo funcionamiento interno no puede ver.

La libertad necesita información. Y si el sistema que nos informa también nos perfila, nos ordena y nos predice, entonces la libertad digital exige algo más que botones de configuración.

La nube tiene suelo

Uno de los grandes engaños del lenguaje tecnológico es la palabra “nube”. Parece ligera, limpia, casi mágica. Subimos archivos “a la nube”, entrenamos modelos “en la nube”, guardamos recuerdos “en la nube”. Pero la nube no flota. La nube tiene suelo, cables, servidores, agua, electricidad, hormigón, trabajadores, minerales y territorio.

La huella digital también tiene una huella física.

Según la Agencia Internacional de la Energía, los centros de datos consumieron alrededor de 415 TWh de electricidad en 2024, aproximadamente el 1,5% del consumo eléctrico mundial. Y la misma agencia proyecta que esa cifra podría superar los 900 TWh hacia 2030.

Puede parecer abstracto, pero no lo es: cada búsqueda, cada vídeo, cada recomendación, cada modelo de IA, cada copia de seguridad, cada anuncio personalizado, vive en alguna parte.

La paradoja es evidente. Lo digital se vende como inmaterial, pero depende de infraestructuras cada vez más materiales. Queremos respuestas instantáneas, almacenamiento infinito, inteligencia artificial en todas partes y plataformas siempre disponibles. Pero pocas veces preguntamos cuánto cuesta sostener esa promesa.

- ¿Puede una empresa llamarse sostenible si su negocio depende de expandir indefinidamente el procesamiento de datos?
- ¿Puede hablarse de innovación sin hablar también de energía?
- ¿Puede una sociedad digital ignorar el agua que enfría sus servidores?

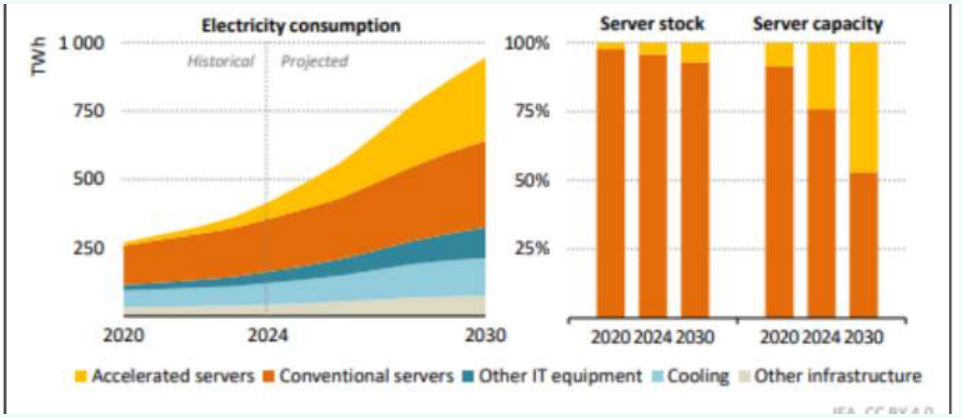


Imagen 3. Consumo eléctrico global de los centros de datos en el escenario base, 2020-2030.

No se trata de demonizar la tecnología. La digitalización también puede ayudar a optimizar redes eléctricas, reducir desplazamientos, mejorar procesos industriales o acelerar investigaciones científicas. Pero el beneficio potencial no cancela el coste real. La huella digital debe medirse completa: no solo en datos recogidos, sino también en recursos consumidos.

La nube no es inmaterial: depende de servidores, refrigeración, infraestructura física y consumo eléctrico. La figura muestra cómo el crecimiento de los centros de datos, especialmente los servidores acelerados asociados a la IA, puede aumentar de forma significativa la demanda energética.

Fuente: International Energy Agency. (2025). Energy and AI. IEA, París. Licencia CC BY 4.0.

El poder de las puertas

La Unión Europea ha llamado “gatekeepers” a varias grandes empresas tecnológicas: guardianes de acceso. La palabra es importante. No describe simplemente empresas grandes; describe empresas que controlan puertas.

Una puerta puede ser un sistema operativo, una tienda de aplicaciones, un buscador, una red social, una plataforma de vídeos, un marketplace o una infraestructura cloud. Quien controla la puerta no solo participa en el mercado: decide las condiciones de entrada. Aquí la huella digital adquiere una dimensión política. Porque si unas pocas empresas concentran la atención, los datos, la infraestructura y los canales de distribución, su poder deja de ser solo económico. Se vuelve cultural, informativo y social.

No es lo mismo vender zapatos que organizar el espacio donde millones de personas descubren qué zapatos existen. No es lo mismo publicar vídeos que decidir qué vídeos llegan a la pantalla de cada usuario. No es lo mismo ofrecer almacenamiento que sostener la infraestructura digital de miles de empresas, administraciones y servicios.

Las grandes empresas tecnológicas no son simples actores dentro de internet. En muchos casos, son parte del propio terreno donde internet ocurre.

Por eso el debate sobre la huella digital no puede limitarse a “proteger mi privacidad”. Eso es necesario, pero insuficiente. La cuestión es más amplia y tiene preguntas más complejas como: ¿qué tipo de sociedad se construye cuando la experiencia cotidiana está mediada por plataformas que convierten nuestras acciones en datos y nuestros datos en ventaja competitiva?

Las grandes plataformas digitales no solo acumulan datos: controlan puertas de acceso a mercados, información, aplicaciones, publicidad, redes sociales y sistemas operativos.

Imagen 3. Gatekeepers designados por la Comisión Europea bajo el Digital Markets Act.

Esta imagen muestra los principales gatekeepers y los servicios de plataforma esenciales asociados a cada uno.

Fuente: Comisión Europea. (2025). DMA Gatekeepers Portal – Gatekeeper Designations.

La responsabilidad que no cabe en una política de privacidad

Las empresas suelen responder a estas críticas con políticas de privacidad, informes de sostenibilidad, controles de usuario y promesas de transparencia. Todo eso importa. Pero también tiene límites.

Una política de privacidad puede informar, pero no necesariamente equilibrar el poder. Un botón de configuración puede ofrecer control, pero no explicar el sistema. Un informe de sostenibilidad puede mostrar avances, pero también seleccionar qué métricas se enseñan y cuáles quedan fuera.

El verdadero problema es que la responsabilidad corporativa suele llegar después de la arquitectura. Primero se diseña el sistema para captar atención, datos y rendimiento; después se añaden capas de consentimiento, auditoría o cumplimiento normativo.

Esto crea el mismo dilema de siempre: optimizar o proteger.

- Optimizar la publicidad o proteger la intimidad.
- Optimizar la retención o proteger la autonomía.
- Optimizar la infraestructura o proteger el planeta.
- Optimizar el crecimiento o proteger la democracia informativa.

Y aquí conviene ser honestos: las grandes empresas no son villanos de caricatura. No hace falta imaginar una conspiración oscura para comprender el problema. Basta con observar los incentivos.

Si el modelo de negocio premia la captura de atención, se diseñarán sistemas para capturar atención. Si se premia la predicción de conducta, se acumularán datos para predecir conducta. Si premia la escala, se construirá infraestructura para escalar. Por ende, queda claro que el peligro no está en una maldad excepcional, sino en una normalidad optimizada.

El rastro también nos mira

La huella digital parece algo que dejamos atrás, pero en realidad también camina delante de nosotros.

Anticipa lo que podríamos comprar, mirar, creer, rechazar o desear. Se convierte en una sombra predictiva que las grandes empresas usan para organizar mercados, anuncios, recomendaciones e infraestructuras.

El problema no es tener tecnología. El problema es aceptar sin reflexión que toda experiencia humana deba convertirse en dato, que todo dato deba convertirse en perfil y que todo perfil deba convertirse en beneficio. No podemos vivir fuera de lo digital. Ni tendría sentido intentarlo. Pero sí podemos exigir otra relación con la tecnología: más transparente, más limitada, más responsable y menos extractiva.

Quizá la pregunta final no sea si tenemos huella digital, ya que queda obvio que la tenemos, todos la tenemos. La pregunta importante realmente es: ¿seguirá siendo nuestra o terminará perteneciendo, en la práctica, a quienes mejor saben explotarla?

Porque el futuro digital no se decidirá solo por la inteligencia de los algoritmos, sino por los límites que seamos capaces de ponerles a las empresas que los utilizan.

La huella está ahí.

El dilema es si aprenderemos a verla antes de que otros decidan por nosotros qué significa.

RUBÉN VALVERDE ROMERO

El Algoritmo Psicológico: CÓMO TU HUELLA DIGITAL PREDICE TU SOLVENCIA Y PERPETÚA LA DESIGUALDAD

Estamos presenciando el ocaso de la "nómina estática" como único tótem de la fiabilidad financiera. El acceso al capital ya no depende exclusivamente de un balance histórico de ingresos y deudas; hoy, el fantasma digital en la máquina decide en silencio quién pertenece a la aristocracia del crédito. El eje financiero ha pivotado hacia el "comportamiento fluido": un análisis en tiempo real donde la forma en que interactuamos con nuestras pantallas pesa más que un contrato de trabajo tradicional.

La premisa parece un ejercicio de determinismo estadístico: "Compartir un botellón en redes sociales te puede dejar sin hipoteca". No es una exageración distópica, sino la realidad de los datos alternativos. Los algoritmos evalúan la impulsividad y el orden personal a través de microcomportamientos que escapan a los registros tradicionales. Esta vigilancia invisible busca un orden matemático en nuestra psicología profunda, bajo la premisa de que nuestros clics nocturnos ofrecen una ventana más honesta a nuestra estabilidad que un extracto bancario pulido.

El Impuesto Cognitivo: La Neurociencia de la Escasez

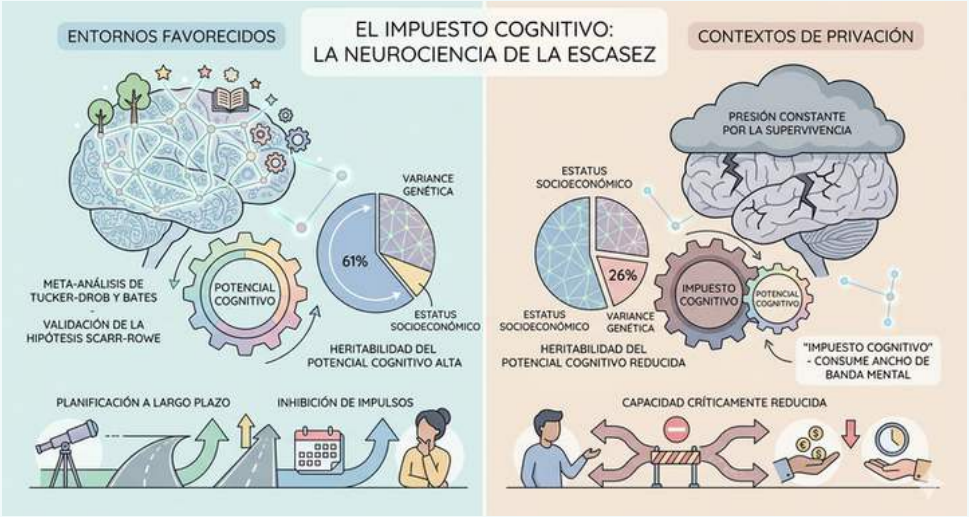
El riesgo crediticio no es una cifra abstracta, sino el resultado directo de un entorno socioeconómico que altera el desarrollo cerebral humano. La neurociencia conductual demuestra que la pobreza no es solo falta de recursos materiales; es un factor ambiental agresivo que actúa como supresor del potencial biológico.

El estudio meta-analítico de Tucker-Drob y Bates (casi 50.000 individuos) validó la Hipótesis Scarr-Rowe: la varianza genética en la inteligencia es un rehén del estatus socioeconómico (SES). En entornos favorecidos, la heritabilidad del potencial cognitivo alcanza un 61%, mientras que en contextos de privación se desploma al 26%.

El SES como Supresor del Potencial (Meta-análisis de gemelos)

Contexto Geográfico	Interacción Genética x SES	Consecuencia Biológica
Estados Unidos	Alta y significativa (26% vs 61%)	Supresión del potencial genético en la pobreza
Europa Occidental / Australia	Nula o inversa	Expresión genética homogénea por políticas de bienestar.

Este impuesto cognitivo se manifiesta físicamente en cada rastro digital que los algoritmos de riesgo ahora rastrean con voracidad.



La escasez impone un "impuesto cognitivo": la presión constante por la supervivencia consume el ancho de banda mental, dejando al individuo con una capacidad reducida para la planificación a largo plazo o la inhibición de impulsos.

La Huella de la Conducta: Del Estado Mental al Rastro Digital

La psicología de la gratificación instantánea, exacerbada por el estrés de la escasez, alimenta los modelos predictivos de las fintech. Cuando el ancho de banda mental está saturado por la incertidumbre, emergen patrones de impulsividad que el algoritmo interpreta como "alto peligro". El clic compulsivo en redes a deshoras o el consumo emocional no son malos hábitos, sino síntomas visibles de una biología bajo presión extrema.

Para capturar esta vulnerabilidad, se emplean técnicas de device fingerprinting. Ya no importa solo lo que compras, sino cómo lo haces: el modelo del teléfono, la velocidad del

tecleo, el nivel de batería o la estabilidad de la conexión se convierten en indicadores de estabilidad personal. Aquí reside la ironía: lo que el algoritmo penaliza como "irresponsabilidad" es la manifestación conductual inevitable de un cerebro bajo el impuesto cognitivo de la pobreza.

La Cosecha Silenciosa: El Mercado de Sombras de los Data Brokers

Estos síntomas psicológicos llegan a los analistas a través de la infraestructura de datos moderna. Los data brokers (intermediarios de datos) procesan la "huella exhausta": el residuo digital de nuestra vida conectada, como el historial de navegación, los likes y la geolocalización. Ellos transforman metadatos triviales en activos financieros de alta precisión.

A través de puentes invisibles, estos intermediarios fusionan datos financieros tradicionales (como el historial de morosidad o la antigüedad de las cuentas) con las variables conductuales recogidas en la red. La supuesta despersonalización del dato es un velo tenue. El algoritmo no necesita un nombre; le basta con deconstruir los patrones temporales de navegación y consumo para inferir una identidad financiera única y predecir la conducta del usuario.

El Veredicto de la Máquina: Del Scorecard Tradicional a la IA

Para transformar la conducta digital en una puntuación de riesgo, el sector financiero ha evolucionado su motor estadístico. Tradicionalmente, los bancos recurrían a los Scorecards basados en la transformación Weight of Evidence (WoE), que establece una relación lineal con las probabilidades de impago.

Esta agrupación hacía que los valores atípicos desaparecieran en categorías manejables, pero generaba exclusión: si un individuo tenía un historial digital "delgado" (thin file) debido a su exclusión tecnológica, el WoE lo agrupaba automáticamente en el nivel de mayor riesgo.

Hoy, la rigidez analítica ha dado paso a arquitecturas híbridas LSTM-XGBoost y Foundation Models, capaces de capturar dependencias temporales complejas. El hábito se traduce en destino mediante el cálculo de la Probability of Default en tiempo real (PIT-ness), una métrica que evalúa el riesgo en el "aquí y ahora", despojando al análisis de consideraciones humanas.

Mediante el Monotonic Binning y la regresión isotónica, los analistas aseguran que la relación entre el predictor y el impago sea constante. A través del Valor de Información (IV), el sistema mide qué tan predictivo es un hábito. Si detecta desvelos recurrentes, no emite un juicio moral, sino un coeficiente de inestabilidad.

El veredicto es de una frialdad absoluta: la correlación técnica sustituye a la causalidad humana.

El Bucle de la Desigualdad Algorítmica

La implementación masiva de estos sistemas choca de frente con las fairness metrics (métricas de equidad), desvelando una preocupante exclusión automatizada. El peligro real no es que la Inteligencia Artificial cometa errores de calculo, sino que mide con precisión el síntoma erróneo: está etiquetando la escasez y llamándola insolvencia.

Al penalizar variables como el uso intensivo de las líneas de crédito o la inestabilidad conductual derivada del estrés financiero, los algoritmos actúan como un techo de hormigón para las clases desfavorecidas.

En Europa Occidental y Australia, donde las redes de seguridad son robustas, el efecto Scarr-Rowe desaparece. Esto demuestra que el sesgo no es un defecto matemático inevitable, sino el reflejo de una infraestructura social fallida.

Al denegar capital por métricas de "inestabilidad" causadas por la propia necesidad, la automatización construye un bucle cerrado donde la pobreza es un error estadístico autocumplido. El sistema congela al individuo en su etapa de potencial suprimido, impidiendo que el crédito actúe como catalizador para la movilidad social.

Estamos diseñando un porvenir donde la máquina no se limita a predecir el riesgo; lo fabrica y lo perpetúa, convirtiendo la falta original de oportunidades en una etiqueta permanente.

SANDRA ESPIÑEIRA BRICEÑO

Your privacy as a product:

THE HIDDEN BUSINESS OF DIGITAL FOOTPRINTS

"If a service is free, you are probably the product." This popular phrase perfectly describes the reality of today's digital world. Every search we make, every "like", every shared location, and every second spent on social media leaves a digital trace behind. Even though these actions may seem harmless or ordinary, they generate a huge amount of information that large technology companies constantly collect and analyse.

We currently live in a hyperconnected society. Applications, social media platforms and smart devices are part of our everyday routines. From the moment we unlock our phones in the morning until we close an app before going to sleep, we are producing data. The real issue is not only the amount of information we share, but also the economic value that this information has for companies.

Today, technology companies no longer only sell products or services; they sell predictions about our behaviour. Our habits, interests and preferences have become one of the most valuable resources in the digital economy.

Every click leaves a mark

A digital footprint is the collection of data and information a person leaves behind while using the internet. Most of the time, we are not fully aware of it, but almost everything we do online contributes to building our digital identity.

There are two main types of digital footprints: active and passive.

An active digital footprint is created intentionally. Posting pictures on social media, writing comments, filling out online forms, or sharing opinions are clear examples of information users choose to make public. Platforms such as Instagram, TikTok and LinkedIn constantly rely on this type of content.

On the other hand, a passive digital footprint is much more invisible. It is automatically generated while browsing the internet. This includes cookies, real-time location tracking, browsing history, screen time or even the speed at which we scroll through content.

Companies such as Google, Meta, Amazon and TikTok collect enormous amounts of information through these systems. By using advanced algorithms, they can analyse behavioural patterns and create highly detailed profiles of millions of users.

In many cases, users do not realise how much they are being digitally monitored. Most people accept terms and conditions without reading them, prioritising convenience over privacy.

The business behind our data

The massive collection of personal data does not happen by accident. Behind it lies one of the most profitable business models in the digital world: the monetisation of personal information.

Digital platforms constantly analyse our behaviour to provide hyper-personalised advertising. Every search, interaction or purchase helps improve algorithms capable of predicting what we want to consume, when we want it and how likely we are to engage with it.

This explains why, after searching for a product or even talking about it, related advertisements suddenly begin to appear across different apps and websites. Although many people consider this a coincidence, it is actually the result of complex data-tracking and advertising systems.

However, companies are not only selling advertising. They are selling access to our attention. In what is known as the "attention economy", the time users spend online becomes a source of profit. The longer users stay on a platform, the more data they generate and the more money companies earn. This is why many social media platforms and applications are specifically designed to keep people connected for as long as possible.

Constant notifications, automatic recommendations and infinite scrolling are not random features. Behind them are psychological studies and algorithms created to capture and maintain user attention continuously. TikTok is one of the clearest examples of this phenomenon. Its algorithm quickly learns what type of content attracts each user and adapts the feed accordingly, keeping users engaged for hours. Similar strategies can also be seen on Instagram, YouTube and Netflix, where personalised recommendations significantly increase screen time. In addition, companies use collected information to build psychological and consumer profiles. These profiles help predict behaviours, political interests, shopping habits and even emotional states.

Data has become such a valuable resource that many companies base a large part of their economic power on their ability to collect, analyse and commercialise personal information.

The invisible cost of personalisation

Personalisation can certainly feel useful and convenient. Receiving recommendations adapted to our interests saves time and improves the user experience. However, this convenience comes with a silent cost: the gradual loss of privacy.

Every time an algorithm learns more about us, its ability to influence our decisions also increases. Digital platforms do not simply show content based on our preferences; they also shape the information we consume every day.

This often creates what are known as “filter bubbles”, where users are mainly exposed to content that matches their beliefs and interests. As a result, diversity of opinions decreases and social polarisation increases. Another major issue is behavioural manipulation. Many platforms use systems specifically designed to create digital dependency.

Notifications, instant rewards and endless recommendations constantly stimulate the need to continue consuming content.

Most people have experienced opening an app “for just five minutes” and then realizing they have spent more than an hour scrolling without noticing the time passing. This design is not accidental. Algorithms can also reproduce existing biases and inequalities. Depending on the data they are trained with, some systems may favour or disadvantage certain groups without users even being aware of it.

Another important concern is the permanence of information online. Pictures, comments or old posts can remain available for years and may affect both personal and professional reputations. Today, many companies review the candidates' online presence before hiring them. Our digital footprint has become part of our public identity.

Are we accepting too much?

The rise of the digital economy has sparked a significant ethical debate about privacy and the use of personal data. While many platforms claim to act transparently, in reality, most users don't fully understand what information they share or how it will be used.

Automatically accepting cookies and privacy policies has become a habit. Most people prioritise quick access to services over reading lengthy and complex privacy agreements.

In response to these concerns, international organisations have introduced regulations intended to protect users. One of the most important examples is the General Data Protection Regulation (GDPR) introduced by the European Union. Its objective is to provide users with more control over their personal data and require greater transparency from technology companies.

However, the rapid development of technology continues to challenge current regulations. Artificial intelligence tools, facial recognition systems and predictive algorithms are constantly expanding the possibilities of data collection.

The key question remains: are we accepting digital conditions without truly understanding the price? Beyond regulations, there is also an individual and social responsibility. Digital literacy has become essential to understanding how the platforms we use daily actually work and what consequences the constant exchange of data can have.

Being aware of the value of our information is the first step towards making more responsible digital decisions.

The real price of being connected

We live in a world where information is more valuable than ever before. Large technology companies have built billion-dollar business models based on collecting and analysing personal data. Every click, search and interaction feeds systems capable of understanding our habits with increasing precision.

Digital convenience clearly offers many advantages. Through personalisation, platforms can provide relevant content, improve services and simplify everyday tasks. However, society has also normalised sharing enormous amounts of information without fully considering the consequences.

In today’s digital economy, personal data has become a form of currency. The real question is no longer how much companies know about us, but how much we are willing to sacrifice in exchange for convenience, connection and entertainment.

Because, in the end, if something appears completely free on the internet, the real product is probably
us.

SANDRA GUTIERREZ DE TENA

La huella digital desde la infancia:

CRECER EN INTERNET ANTES DE APRENDER A PROTEGERSE LA PRIMERA GENERACIÓN QUE NACE CONECTADA

Hace apenas unos años, la mayoría de las personas comenzaban a construir su identidad digital en la adolescencia o incluso en la adultez. Hoy, en cambio, muchos niños tienen presencia en internet incluso antes de nacer. Fotografías de ecografías compartidas en redes sociales, vídeos familiares publicados en plataformas digitales o perfiles creados por sus propios padres forman parte de una nueva realidad: la construcción de una huella digital desde la infancia.

La huella digital es el conjunto de datos, imágenes, comentarios e información que dejamos en internet de manera consciente o inconsciente. Cada publicación, búsqueda, fotografía o interacción online genera un rastro que puede permanecer durante años.

El problema es que, en el caso de los niños pequeños, gran parte de esa información es compartida por adultos antes de que los niños puedan decidir por sí mismos qué quieren mostrar al mundo.

Este fenómeno ha abierto un debate cada vez más importante dentro de la ciberseguridad y la privacidad digital. ¿Qué consecuencias tendrá crecer con una identidad digital creada desde la infancia? ¿Quién controla esos datos? ¿Y qué riesgos existen cuando empresas tecnológicas, plataformas educativas y redes sociales almacenan información de menores durante años?

Sharenting: cuando la infancia se convierte en contenido

Para empezar, uno de los conceptos más relevantes en este debate es el sharenting, una combinación de las palabras inglesas share (compartir) y parenting (crianza). El término hace referencia a la práctica de padres y familiares que publican constantemente fotografías, vídeos e información sobre sus hijos en internet.

Aunque muchas veces estas publicaciones tienen una intención inocente (compartir momentos familiares, celebrar logros o mantener contacto con amigos y familiares, etc), también generan enormes cantidades de información personal accesible para empresas y, en algunos casos, para desconocidos.

Un niño puede aparecer en cientos de fotos antes de cumplir cinco años. Algunas de esas imágenes incluyen datos sensibles: nombre completo, colegio, ubicación, rutinas diarias o incluso información médica. Lo preocupante es que esos contenidos pueden permanecer online indefinidamente, incluso después de haber sido eliminados.

Las redes sociales recopilan metadatos de cada publicación: fecha, localización, dispositivos utilizados y patrones de comportamiento. En otras palabras: no solo se comparte una fotografía, también se entrega información valiosa que puede ser utilizada para fines comerciales, algoritmos publicitarios o análisis de comportamiento.

Además, muchos menores no tienen capacidad para consentir esa exposición pública.

Cuando crezcan, podrían descubrir que gran parte de su vida ya estaba documentada en internet sin haber participado en la decisión.

Las grandes empresas y el valor de los datos infantiles

En la economía digital actual, los datos personales se han convertido en uno de los activos más valiosos del mundo. Las grandes empresas tecnológicas recopilan información constantemente para desarrollar perfiles de usuarios, personalizar publicidad y mejorar algoritmos.

En el caso de los menores, aunque sea preocupante, el interés empresarial existe. Cuanto antes una plataforma consigue datos de una persona, más fácil resulta analizar sus hábitos, gustos y comportamientos futuros.

Aplicaciones móviles, videojuegos, plataformas educativas y redes sociales recopilan información como:

- Tiempo de uso.
- Ubicación.
- Preferencias de contenido.
- Interacciones sociales.
- Historial de navegación.
- Datos biométricos.
- Voz e imágenes.

Muchas aplicaciones dirigidas a niños solicitan permisos excesivos para acceder al micrófono, la cámara o la geolocalización. Aunque parte de esta información se utiliza para mejorar el funcionamiento de las plataformas, otra parte se emplea para crear modelos de comportamiento extremadamente precisos.

La preocupación aumenta cuando estos datos se almacenan durante años o se comparten con terceros. Un perfil digital construido desde la infancia podría acompañar a una persona durante toda su vida.

Plataformas educativas: aprendizaje y vigilancia digital

La pandemia aceleró la digitalización de la educación y convirtió las plataformas virtuales en herramientas esenciales para millones de estudiantes. Sin embargo, este cambio también incrementó la recopilación masiva de datos de menores.

Muchas plataformas educativas registran:

- Horarios de conexión.
- Actividades realizadas.
- Resultados académicos.
- Tiempo de atención.
- Participación en clase.
- Interacciones con profesores y compañeros.

Estos sistemas generan enormes bases de datos sobre comportamiento infantil y rendimiento escolar. Aunque la tecnología educativa ofrece ventajas importantes, también plantea dudas sobre privacidad y seguridad.

¿Quién tiene acceso a esa información? ¿Durante cuánto tiempo se almacena? ¿Podría utilizarse en el futuro para evaluar oportunidades académicas o laborales?

Expertos en ciberseguridad advierten que los menores son especialmente vulnerables porque no comprenden completamente cómo funcionan estas plataformas ni las

consecuencias de compartir datos personales. Además, las instituciones educativas suelen ser objetivos atractivos para los ciberdelincuentes. En los últimos años se han producido ataques a colegios y universidades.

Riesgos futuros de una identidad digital temprana

Uno de los mayores problemas de la huella digital infantil es que sus consecuencias reales pueden aparecer muchos años después.

Una fotografía aparentemente inocente publicada durante la niñez podría afectar la reputación personal o profesional en la adultez. Empresas, universidades y organizaciones revisan cada vez más la presencia online de las personas antes de tomar decisiones importantes.

La información compartida en internet también puede ser utilizada para:

- Robo de identidad.
- Suplantación de perfiles.
- Estafas digitales.
- Ciberacoso.
- Ingeniería social.
- Extorsión.

La ingeniería social es especialmente peligrosa porque utiliza información personal para manipular o engañar a las víctimas. Cuantos más datos existan sobre una persona, más fácil resulta diseñar ataques convincentes.

Por ejemplo, un ciberdelincuente podría utilizar información pública sobre el colegio, amigos o actividades de un menor para realizar ataques de phishing personalizados.

El problema del consentimiento digital

Uno de los aspectos más complejos de este tema es el consentimiento. Los niños pequeños no comprenden completamente qué implica tener presencia online ni cómo se utilizan sus datos.

Sin embargo, muchas plataformas permiten la recopilación de información mediante políticas de privacidad extensas y difíciles de entender incluso para adultos.

Los padres, por su parte, suelen aceptar términos y condiciones sin leer completamente cómo serán utilizados los datos de sus hijos. Esto genera una situación paradójica: la identidad digital de un niño puede ser explotada comercialmente antes de que tenga edad suficiente para comprender internet.

Algunos expertos consideran que la sociedad todavía no ha desarrollado normas claras sobre privacidad infantil en el entorno digital. Aunque existen regulaciones como el Reglamento General de Protección de Datos (RGPD) en Europa, la velocidad del desarrollo tecnológico supera con frecuencia la capacidad de adaptación legal.

Redes sociales y presión por compartir

Las redes sociales han transformado la forma en que las personas construyen su identidad. Publicar contenido se ha convertido en una práctica cotidiana y, en muchos casos, socialmente incentivada.

Muchos padres sienten presión por compartir momentos familiares:

- Cumpleaños.
- Primer día de colegio.
- Vacaciones.
- Actividades deportivas.
- Logros académicos.

El problema aparece cuando la vida privada de los menores se convierte en contenido permanente para internet. En algunos casos extremos, incluso existen familias que monetizan la exposición de sus hijos mediante vídeos en, por ejemplo, youtube, o perfiles con millones de seguidores.

Esto ha generado debates éticos sobre los límites entre la vida familiar y la explotación de la imagen infantil en plataformas digitales.

Además, una vez que una foto o vídeo se publica online, el control sobre ese contenido disminuye enormemente.

Las imágenes pueden descargarse, compartirse, copiarse o almacenarse en servidores externos sin conocimiento de la familia.

Educación digital: una necesidad urgente

Ante todo lo explicado y la situación actual, la educación digital debe comenzar desde edades tempranas.

No se trata únicamente de enseñar a utilizar dispositivos tecnológicos, sino de comprender:

- Qué es la privacidad.
- Cómo funcionan los datos personales.
- Qué riesgos existen en internet.
- Cómo proteger cuentas y perfiles.
- Qué información no debería compartirse públicamente.

Esto también debe incluir a los adultos. Muchos padres desconocen el alcance real de las publicaciones que realizan sobre sus hijos, siendo muchas veces el principal problema de que la información de sus hijos quede expuesta en internet. Configurar correctamente la privacidad de las redes sociales, limitar la información visible públicamente y evitar compartir datos sensibles son medidas básicas que pueden reducir significativamente los riesgos.

¿Es posible borrar la huella digital?

Una de las grandes características de internet es su capacidad para almacenar información durante largos periodos de tiempo. Aunque algunos contenidos pueden eliminarse, no siempre desaparecen completamente. Copias de seguridad, archivos digitales y capturas de pantalla hacen que la eliminación total sea extremadamente difícil.

Por ello, muchos especialistas recomiendan aplicar el principio de pensar antes de publicar. Cada fotografía o dato compartido sobre un menor debería evaluarse considerando si podría afectarle en el futuro.

La pregunta ya no es solamente qué compartimos, sino cuánto control conservamos sobre esa información una vez entra en el ecosistema digital.

El desafío de proteger la infancia en la era digital

La tecnología ofrece enormes beneficios educativos, sociales y culturales para los niños pequeños. El problema no es internet en sí, sino el uso irresponsable de los datos personales y la falta de conciencia sobre sus consecuencias. La primera generación que crece completamente conectada enfrenta un desafío único: construir su identidad en un entorno donde cada acción puede quedar registrada permanentemente.

La huella digital infantil no es solo un asunto de privacidad, también es una cuestión de seguridad, derechos y futuro. Las decisiones tomadas hoy por padres, empresas y gobiernos influirán directamente en cómo millones de niños vivirán su relación con internet en los próximos años.

En una sociedad cada vez más digitalizada, proteger la información de los menores se ha convertido en una responsabilidad colectiva. Porque, detrás de cada dato almacenado, existe una persona que todavía no ha tenido la oportunidad de decidir cómo quiere ser vista por el mundo.

VICTOR ASUNCIÓN

TU HUELLA EN INTERNET VALE DINERO Y NO ES PARA TI

Cada vez que abres Instagram por la mañana, buscas algo en Google o aceptas las cookies de una página web, estás dejando un rastro. Un rastro que no desaparece, que se almacena, se procesa y, en la gran mayoría de los casos, se convierte en dinero. El problema no es solo que esto ocurra, sino que ocurre con nuestro consentimiento, aunque sin nuestro conocimiento real.

Bienvenido a la economía de los datos, uno de los negocios más rentables del siglo XXI.

¿Qué es exactamente tu huella digital?

Tu huella digital es el conjunto de datos que generas cada vez que interactúas con cualquier plataforma o servicio en línea. No hablamos solo de lo que publicas conscientemente: también incluye cuánto tiempo te quedas mirando una publicación, a qué hora te conectas, qué dispositivo usas, desde dónde lo haces, qué compras, qué buscas y qué no llegas a comprar. Cada clic, cada scroll, cada búsqueda forma parte de un perfil tuyo que se construye en tiempo real y con una precisión que, probablemente, te sorprendería.

Lo que hace especialmente valioso a este perfil no es ningún dato concreto por sí solo, sino la combinación de todos ellos. Saber que alguien tiene 23 años vale poco. Saber que esa persona de 23 años busca apartamentos, ha visitado páginas de ofertas de empleo en los últimos días, usa el móvil principalmente de noche y ha comprado libros de finanzas personales, ya es otra cosa. El Big Data permite analizar tendencias económicas, políticas, de ocio, sanitarias e incluso emocionales de cada individuo a partir de datos aparentemente básicos. Lo que para nosotros es rutina digital, para las plataformas es señal. Y esas señales, agrupadas y analizadas, tienen un valor comercial enorme.

El negocio detrás de la pantalla

Las grandes plataformas digitales llevan años construyendo su modelo de negocio sobre una premisa muy sencilla: si el servicio es gratis, el producto eres tú. Meta, Google, TikTok o Amazon no cobran por usar sus servicios porque no lo necesitan. Lo que monetizan es el acceso a ti, o más concretamente, al perfil detallado que han construido sobre ti.

> *"Si el servicio es gratis, el producto eres tú. Lo que venden no es publicidad: venden acceso a una versión digitalizada de quién eres."*
> *– ECONOMÍA DE LOS DATOS · SIGLO XXI*

El mecanismo principal es la publicidad segmentada y, más concretamente, lo que se conoce como publicidad programática. A través de sistemas de pujas en tiempo real —los llamados Real Time Bidding—, las marcas pujan automáticamente en función de los datos de los usuarios en apenas medio segundo, consiguiendo que el anuncio correcto llegue a la persona correcta en el momento exacto. No es un anuncio para "mujeres de 18 a 35 años": es un anuncio para alguien que ha buscado zapatillas de running en los últimos tres días, tiene un nivel de gasto medio-alto y suele conectarse a las 22 h.

En Estados Unidos, el gasto en publicidad programática se estimaba en 168.000 millones de dólares en 2024, lo que da una idea real de la magnitud económica de este mercado. Esa cifra no viene de la nada: viene de ti, de mí y de cada usuario que cada día deja rastros digitales sin ser del todo consciente de su valor.

Los intermediarios del dato

Pero la publicidad es solo la capa más visible del negocio. Más allá de ella existe toda una industria paralela: la de los data brokers o intermediarios de datos. Son empresas cuyo modelo de negocio consiste, literalmente, en recopilar, procesar y vender información sobre personas.

Obtienen y analizan datos de múltiples fuentes para determinar todo tipo de información personal: desde datos de identificación y demográficos hasta información financiera, de vivienda o de salud.

El retrato robot de miles de personas puede venderse por menos de diez céntimos cada uno. Sin embargo, sumando la facturación de los principales data brokers, se obtiene una cifra de 8.500 millones de euros al año. La clave, como suele ocurrir en los negocios más rentables, no está en el precio unitario, sino en el volumen.

$168B
GASTO GLOBAL EN PUBLICIDAD PROGRAMÁTICA (2024, EE.UU.)

€8.5B
FACTURACIÓN ANUAL ESTIMADA DE LOS PRINCIPALES DATA BROKERS

3%
CONSUMIDORES QUE SIENTEN CONTROL REAL SOBRE SUS DATOS ONLINE

Lo que aceptamos sin leer

Aquí es donde el modelo se vuelve especialmente revelador desde un punto de vista de negocio. Todo lo anterior es, técnicamente, legal. Cuando instalas una aplicación o entras en una web, aparece una política de privacidad y unos términos y condiciones que, en teoría, explican exactamente qué datos se recogen y para qué se usan. El problema es que leerlos no está al alcance de casi nadie: se estima que leer los términos y condiciones de todos los servicios que usa una persona media llevaría varias semanas completas al año.

De media, solo entre instalaciones de apps, registros médicos y compras en comercios, una persona acepta más de 40 consentimientos de uso de datos personales al año. El resultado es un consentimiento que existe en papel, pero que no lo es en la práctica.

Una generación de datos

Algunos data brokers se jactan de no vender datos a terceros. Lo que sí hacen es vender el acceso a esos datos, que para el caso es exactamente lo mismo. Aceptamos porque no queda otra, porque queremos acceder al servicio, y porque el sistema está diseñado exactamente para eso. No es un fallo del sistema: es el sistema.

Los que crecimos con un smartphone en la mano somos, probablemente, la generación más perfilada de la historia. Hemos dejado rastros digitales desde la adolescencia. Regulaciones como el RGPD en Europa han supuesto un avance real, reconociendo derechos como saber qué datos tienen sobre ti, corregirlos o solicitar su eliminación. Sin embargo, solo el 3% de los consumidores siente que tiene control real sobre sus datos en línea. No se trata de dejar de usar internet ni de dejar de usar internet ni de caer en el alarmismo. Se trata de algo más sutil: ser conscientes del intercambio que estamos haciendo. Cada vez que usamos un servicio gratuito, estamos pagando con algo que tiene un valor real, aunque no veamos el precio en ninguna pantalla. Lo que para nosotros es rutina —un clic, una búsqueda, una foto— para ellos es una señal. Y esas señales, agrupadas, valen dinero real.

La pregunta que queda abierta es si ese intercambio es justo. Si la información disponible es suficiente para que sea una decisión real y no una aceptación por defecto. Y si, como sociedad —y especialmente como generación que ha normalizado compartirlo todo—, queremos seguir siendo la materia prima de uno de los negocios más rentables del mundo sin recibir nada a cambio, más allá de poder seguir scrolleando gratis.

MSMK magazine

MSMK University College