

## Ofuscación de datos: si no puedes evitar que te rastreen, engaña al algoritmo

📅 27.03.2021



Proyección de datos de Twitter, Instagram y Transportes de Londres a cargo del estudio Tekija para la exposición Big Bang Data en Londres en 2019. Getty

Vivir en la era digital significa ser rastreado continuamente. Nuestras actividades cotidianas dejan [una huella en el ciberespacio](#) que, debidamente procesada, ayuda a las empresas a vendernos sus productos. El pacto implícito es el siguiente: los usuarios accedemos gratis a que las empresas recopilen nuestros datos a cambio de la promesa de recibir mejores servicios. Pero no todo el mundo está dispuesto a ceder a la ligera su información personal para que otras empresas se lucren con ella. Que lo sepan todo sobre nosotros puede suponer una [vulneración de la privacidad](#) de los individuos, y además puede resultar molesto ser perseguido por anuncios y ofertas a todas horas.

¿Hay forma de escapar al escrutinio de las empresas tecnológicas? Es muy difícil, sobre todo si usamos sus servicios a diario. Pero hay una manera de expresar la rebeldía desde dentro el sistema: ofrecer datos incorrectos para confundir a quienes los recopilan. Una forma sencilla de hacerlo sería dar nombre y dirección falsas cuando se le pide a uno esa información para registrarse en alguna página web; otra más elaborada sería usar programas especiales que pinchen automáticamente en todos los *banners* que se nos ofrezcan, de manera que resulte difícil inferir nuestros gustos. A esto se le llama ofuscación de datos y, si lo practicase una masa crítica de gente lo suficientemente amplia, el *big data* acabaría por ser irrelevante. Porque los algoritmos, sin datos de calidad, no sirven para nada.

La industria es consciente del poder de esta práctica. Tanto es así que la consultora Gartner incluyó el *algorithm hacking* (así se le llama también) como [una de las cinco claves a seguir en 2020 en su informe anual de tendencias](#) de consumo para profesionales del marketing. No está claro cuánta gente practica la ofuscación de datos. Según Kate Muhl, analista de Gartner, en torno a una cuarta parte de los consumidores lo hacen en su día a día, aunque sea poniendo un nombre falso al rellenar un formulario online.

Tampoco se puede establecer qué proporción de datos falsos bastaría para hundir al sistema. El tamaño de las bases de datos y la naturaleza de los algoritmos de aprendizaje automático son muy distintos entre sí. Una simulación realizada con un algoritmo de recomendación de películas llevó a unos investigadores a concluir que si el 30% de los usuarios aportaban al sistema datos falsos, la efectividad del mismo caía al 50%.

### Más hastío que activismo

#### ENTRADAS RECIENTES

Koeman: "Me veo entrenador del Barcelona para la próxima temporada"

Florentino Pérez, sobre la Superliga en el diario As: "O hacemos algo pronto o quebrarán muchos clubes"

El PP teme que la polémica de Monasterio e Iglesias alimente la recta final de la campaña de Podemos y Vox

Radiografía del ideario de Ayuso: aborto, ecologismo y subvencionados

Francia devolvió a España casi 16.000 migrantes en solo cinco meses

Pese a tener un nombre pomposo (ofuscación de datos o alteración de algoritmos), aportar información falsa no es un invento reciente. En el ámbito militar, por ejemplo, se practica desde la Antigüedad para confundir al enemigo. "Mentir es muy intuitivo, casi intrínseco al ser humano. Muchos países incluso admiten un derecho a la mentira. En Estados Unidos está la Primera Enmienda y en algunos ordenamientos jurídicos se permite mentir en un juicio para defenderse a uno mismo", explica la filósofa Carissa Véliz, que en su libro *Privacy is Power* (Bantam Press, 2020) sitúa la ofuscación de datos como una de las vías de acción para proteger nuestra privacidad.

"La ofuscación de datos está mucho más extendida de lo que pensamos", opina por su parte Gemma Galdón, directora de la auditoría de algoritmos Éticas Consulting. "Lo que pasa es que más que como un acto de activismo se hace por incomodidad o hastío. Y eso sucede porque en algún momento la ciudadanía rompió su confianza en la tecnología", añade. Mentir cuando se rellena el formulario de inscripción de una tarjeta de fidelización de un comercio o taparse la cara con el abrigo cuando pasamos ante una cámara de seguridad son dos ejemplos de acciones sencillas y muy comunes.

"Se asume que todos los datos aportados de forma voluntaria por la gente tienen un grado de fiabilidad muy bajo. Su valor en el mercado es prácticamente cero", ilustra Galdón. De ahí que lo que se compra caro son los datos que se obtienen de entidades bancarias o de procesos en los que el ciudadano no tiene la libertad de mentir.

La ofuscación de datos es la aportación deliberada de información ambigua, confusa o falsa para interferir en la vigilancia digital y en la recolección de datos", definen Finn Brunton y Helen Nissenbaum en su obra canónica *Obfuscation. A User's Guide for Privacy and Protest* (MIT Press, 2015). Un reciente [estudio elaborado por investigadores de la Northwestern University](#) (Illinois) distingue entre tres formas de confundir a los algoritmos: con huelgas de datos, intoxicar los datos y aportando datos a la competencia.

## 1. Huelga de datos

La primera medida para erosionar el poder del capitalismo de la vigilancia es abstenerse de generar datos o borrar los que se hayan aportado. Esto se consigue eliminando las cuentas de plataformas que no se consideren imprescindibles o instalando herramientas de privacidad.

Los investigadores de la Northwestern University citan como ejemplo los [boicots a Facebook](#) promovidas en EE UU por asociaciones en defensa de los derechos civiles o a Uber cuando se denunciaron casos de [acoso sexual](#) dentro de la compañía.

## 2. Datos intoxicados

Esta segunda modalidad de ofuscación consiste en aportar de forma consciente datos sin sentido, que confundan a quien los recoge. La forma más sencilla de hacerlo es mintiendo. Por ejemplo, dando me gusta a canciones que en realidad odias en un reproductor de música. O inventando una dirección de correo electrónico cada vez que se nos exige dar uno para poder acceder a una web.

Otra vías más compleja consiste en deslumbrar al algoritmo: mandarle una gran cantidad de datos, todos ellos falsos, para que el perfil que construya sobre nosotros sea todavía más impreciso. Hay extensiones para navegadores como AdNauseam que hacen ese trabajo por nosotros. Da clics de forma automática e imperceptible para el usuario en todos los anuncios que se nos muestran cuando navegamos. El objetivo es que Google Ads no consiga procesar toda esa información, que además será errónea. Otra opción es usar TrackMeNot, que lanza búsquedas constantes y aleatorias en Google, de manera que nuestras auténticas preferencias quedan diluidas.

Un grupo de adolescentes estadounidenses dio el año pasado con una ingeniosa forma de [volver loco a Instagram](#). Decidieron compartir una sola cuenta en la red social. Cada vez que alguien del grupo quería entrar solo tenía que pedirle a quien estuviese conectado que reiniciase la sesión. Tras esa petición, la compañía envía automáticamente una contraseña al dispositivo desde el que se solicita. El compinche solo tiene que compartir esa clave con quien quiera incorporarse. El resultado: el algoritmo mostraba fotos de Kobe Bryant, de recetas de repostería, de coches... Nada que ver con las preferencias de ninguno de ellos.

## 3. Alimentar a la competencia

La tercera vía para engañar a los algoritmos consiste en aportar de forma consciente datos al competidor de la plataforma contra la que se quiera protestar. Por ejemplo, subir las fotos que se tengan en Facebook en Tumblr o usar el buscador DuckDuckGo en vez de Google. El objetivo es fomentar la competencia entre plataformas.

Las consecuencias de estas acciones pueden tener efectos en el espacio físico. En verano de 2019, los conductores de Uber y Lyft de Washington se pusieron de acuerdo para subir las tarifas de los trayectos, lo que afecta a su retribución. El mecanismo: apagar simultáneamente las aplicaciones durante unos minutos, de manera que el algoritmo crea que hay pocos conductores y suba así el precio de las carreras, y volverlas a encender luego.

Puedes seguir a EL PAÍS TECNOLOGÍA en [Facebook](#) y [Twitter](#).

Algoritmos Computacionales

Grandes Tecnológicas

Plataformas Digitales

Privacidad Internet

Tecnología

< Prev

Next >

Tecnología

### Acuarela y realidad virtual: el papel de la tecnología en la última trinchera de la animación tradicional

👤 Beton42g 📅 24.04.2021 💬 0

Tecnología

### Amazon Echo Show 10, a prueba: el asistente con pantalla giratoria que te sigue por el hogar

👤 Beton42g 📅 24.04.2021 💬 0

Tecnología

### El arte de la predicción: cómo salvar la experiencia democrática del usuario

👤 Beton42g 📅 24.04.2021 💬 0

Tecnología

### El nieto que inventó el Yayagram para comunicarse con la abuela Felisa

👤 Beton42g 📅 23.04.2021 💬 0

Tecnología

### Un año y siete copias después, todos quieren ser Clubhouse

👤 Beton42g 📅 23.04.2021 💬 0

Tecnología

### Tecnología recupera su 'newsletter'

👤 Beton42g 📅 22.04.2021 💬 0

You must be logged in to post a comment.

Cream Magazine by [Themebeez](#)