Dos personas se dan la mano

Este es el precio de tus datos personales en internet: hasta 850 euros en el mercado negro

Las grandes empresas tecnológicas comercializan información genérica de sus usuarios; otra cosa es lo que hagan los cibercriminales

ARCHIVADO EN: REDES SOCIALES , INTERNET , PROTECCIÓN DE DATOS

GERARD MATEO , @gerardmateo

03.08.2019 00:00 h. 9 min

El asunto de la **privacidad** de los usuarios en **internet** trae cola. Todo el mundo sabe que, cada vez que realiza una búsqueda, se da de alta en una red social y se descarga una aplicación está entregando sus **datos personales** a la empresa proveedora. Lo hace por **voluntad propia** a cambio de **servicios gratuitos**. Tampoco escapa a nadie que una parte del negocio de estas compañías procede de la **comercialización de esta información**, por lo que cada vez más voces reclaman una regulación más específica; incluso sugieren que el usuario perciba una compensación económica por esta cesión. Pero ¿cómo funciona este mercado?, ¿cuánto valen tus datos en la red? Las respuestas te sorprenderán.

Para empezar, **"venta de datos** como tal hay poca". Al menos, ese no es el proceder de las grandes compañías como **Google** y **Facebook**. Lo que existe "son acuerdos para acceder a determinados datos", explica el profesor de la IE Business School **Enrique Dans**. ¿Qué quiere decir esto? Pues que estas empresas **nunca entregarán la identidad de ningún usuario** a los anunciantes. No obstante, las firmas publicitarias pedirán a estos gigantes que pongan sus reclamos a potenciales clientes que, por ejemplo, vivan en Barcelona, midan más de equis centímetros y consulten de modo recurrente páginas deportivas. **"La base de datos nunca sale de Google o Facebook** --tras los escándalos ha reconducido su conducta--, que venden el acceso regulado a esos datos, los explotan; es decir, **comercializan una base de datos, pero no la base de datos"**, añade.

Si una aplicación es gratis...

Con todo, hay que ser precavido. **"Cuando una aplicación es gratis es por algo"**, por algún lado se rentabilizará. El profesor también recomienda echarle un vistazo al acuerdo que suscribe el usuario, por más largo y complicado de entender que sea (un lenguaje demasiado preciso, pero muy necesario para evitar cualquier interpretación). Finalmente, hay que **"tener conciencia de qué es lo que firmas** cuando instalas una aplicación". Porque es posible que la *app* incluya una **cláusula** con la que se permite la cesión de los datos a compañías que quieran saber cuándo estás y cuándo no estás en casa. Mucho ojo. No es lo mismo aceptar las leyes de EEUU que las de Rusia en términos de privacidad. Visto todo esto, **¿nuestros datos valen más en grandes paquetes que en formato individual?** Sí. La venta individual "no es habitual" y tendría que ser "parte de una búsqueda específica a través de una aplicación, un ataque muy definido".

Llegados a este punto conviene saber si cada persona puede **vender sus datos a cambio de dinero**. Está el caso de un chico que substató su información personal en eBay (le ofrecieron unos 350 euros) a modo de experimento, pero más allá de eso "todavía no" hay esta opción. Dans declara que "existe alguna posibilidad, algún sistema de cumplimentación de **encuestas a cambio de regalos** o puntos" o "la entrega de muestras para que el usuario pruebe el producto" y este permita formar parte de un **panel de consumidores** que sí se comercializa. Entonces, **¿es posible poner un valor a nuestros datos, un precio?** Sí, aunque **"es difícil"** y, "seguramente, **el valor sea bastante decepcionante"**. Argumenta: "Esto que dicen 'oh, me deben mucho dinero porque han usado mis datos', pues no. Lo que surge de conocer estos datos es que puedes poner publicidad delante de un estrato sociodemográfico determinado, y si consigues exhibir la publicidad, tienes un porcentaje muy bajito de probabilidades de que esa persona reaccione a ese reclamo, por lo que **el dato en sí vale muy poco, un solo dígito. O menos"**.

La 'dark web'

Otra cosa –matiza– es lo que se hace fuera de la ley. Cita el caso de lo ocurrido con **Cambridge Analytica**: "Legalmente **no puedes segmentar en función de raza ni de religión** ni otras variables" como la ideología o las **tendencias sexuales**. Por otra parte, circulan unas estimaciones de Money Guru de lo que valen los datos personales de los usuarios en la llamada ***dark web***, una red oscura que burla las miradas de las autoridades y en la que es posible desde vender falsificaciones hasta comprar armas y drogas. Algo así como el **mercado negro** virtual. Allí, esta identidad personal completa se intercambia a unos **850 euros por persona** (siendo los datos bancarios los más cotizados, unos 700 euros; las redes sociales solo valen entre 3 y 8 euros, y la cuenta de Amazon Prime, unos 11 euros), pero para ello los ciberdelincuentes han tenido que obtenerla de **modo ilegal**, accediendo a bases de datos para robarlos. En cualquier caso, menos de lo que esperaría el usuario medio.

Por todo ello, en lugares como Virgina (EEUU) han presentado un proyecto de ley para que las **grandes empresas de internet informen** a los usuarios sobre los datos que han recabado y que divulguen su valor, según ha publicado *The New York Times* recientemente. Un estudio de la consultora del economista Robert J. Shaphiro asegura que, en el 2018, el beneficio corporativo que produjo la recolección de datos personales de los estadounidenses fue de 76.000 millones de dólares: si se repartieran entre los usuarios, cada uno cobraría **122 dólares –unos 110 euros–**; si el gobierno cobrase una parte, sería una notable fuente de ingresos. De todos modos, según un estudio –ya obsoleto– del economista Erik Brynjolfsson, en 2012, el beneficio al consumidor por tener servicios gratuitos de internet fue de más de 100.000 millones de dólares.

Los beneficios de la comercialización de los datos

Dans apunta también que si la **comercialización de los datos** está bien hecha **"no tiene demasiados peligros"**. Al contrario, el usuario recibe **publicidad mejor segmentada**, que es lo que quiere en el fondo. Sin embargo, desliza, "lo que está ocurriendo es que la publicidad contextualizada sugiere, sobre todo a los jóvenes, que les están **espiando"**. Los publicistas "han estropeado" una ventaja y han convertido la red en algo "claustrofóbico, persecutorio". Hasta el punto que la mala planificación de la publicidad programática --funciona como una subasta en tiempo real de los huecos para publicidad de una página-- ideada para un momento concreto, se prolonga durante días. Por ejemplo, si alguien busca hoteles en un lugar, puede estar semanas en las que le aparezcan ofertas de alojamientos en esa ciudad, lo que le hace pensar **'Me han visto, me tienen controlado'**, y surgen las psicosis.

Hoy por hoy están apareciendo empresas, todavía emergentes, que se encargan de recolectar, asegurar y vender datos personales de manera voluntaria y lo hacen, como no puede ser de otro modo, por medio de la tecnología **blockchain**. Queda mucho por hacer, pero todos los caminos llevan a una mayor regulación de la comercialización de datos personales y a que los usuarios tengan más control sobre ellos, según el experto en publicidad de Facebook **Andreas Schou**.

Siga las noticias más relevantes de esta sección en el Linkedin de Crónica Global

También recomendamos...

Drogas y falsificaciones, el mayor negocio en el mercado negro de internet

¿Qué es eso de la blockchain?

¿Quiere hacer un comentario?

LO MÁS LEÍDO

1 La incompetencia del Govern insulta a los catalanes

2 La dura vida del espía en patios de colegio

3 Barra libre a desgravar con donaciones a entidades independentistas

4 Pilar Rahola, de paella en paella entre Cadaqués y Waterloo

5 Aluvi de sentencias contra el plan hotelero de Ada Colau

Recibe nuestro newsletter.
Tu correo electrónico...
He leído y acepto las condiciones legales
Suscríbirme ahora
Síguenos
Publicación asociada a: OJD

Copyright © CRÓNICA GLOBAL MEDIA, SL. Todos los derechos reservados