CIENCIA Y TECNOLOGÍA / MUNDO

Internet: ¿Qué hacen con nuestros datos?

El Ciudadano · 14 de junio de 2015

Todos hemos oído alguna vez decir que cuando un producto es aparentemente gratuito, es probable que en realidad lo estemos pagando con datos. Ocurre con las redes sociales, las tarjetas de fidelización de tiendas o supermercados o con un sinfín de aplicaciones que nos ofrecen servicios más o menos relevantes a cambio, solamente, de nuestros detalles personales.

Pero más allá de intuir que nosotros somos el producto, en realidad desconocemos qué se hace exactamente con nuestra información, o en qué consiste y cómo funciona ese pago con datos. En realidad, no es una cuestión sencilla, y cada aplicación cuenta con sus propios procedimientos y lógicas. En el caso de la navegación por **Internet**, por ejemplo, las empresas y prestadores de servicios nos ofrecen de forma gratuita sus motores de búsqueda, páginas webs y servicios asociados, para leer la prensa, consultar la previsión meteorológica, o estar en contacto con otras personas a través de redes sociales o foros. No obstante, cada vez que entramos en una web estamos descargando automáticamente una serie de

microprogramas conocidos como*cookies* que recaban información de nuestra actividad *online* y hacen llegar al propietario de la web visitada información sobre nuestra IP, MAC o IMEI (la matrícula de nuestro dispositivo), el tiempo y forma en que utilizamos un sitio concreto u otros sitios que estén abiertos en el mismo momento, identifica si somos visitantes habituales y qué uso hacemos de la página de Internet, en qué secuencia y cómo accedemos a otros sitios, etcétera. Además, es habitual que diferentes empresas paguen al sitio que visitamos para poder instalarnos sus propias *cookies*, como también lo es que la empresa utilice los datos no solo para sus estudios internos, sino que los venda a terceros.

En realidad, cada vez que visitamos una página con el ordenador, el teléfono móvil o la tableta, recibimos decenas de peticiones de instalación de *cookies*. Somos, pues, el producto porque a cambio de la información que obtenemos proporcionamos detalles sobre nuestra actividad*online* y, a menudo, datos personales como nuestro nombre y ubicación, hábitos, tarjeta de crédito, etcétera, de los que no tenemos forma de controlar dónde acaban. Ante esto, el único recurso de autoprotección es o no aceptar *cookies* y renunciar al servicio, o borrarlas sistemáticamente de nuestro ordenador, algo tan engorroso como limitadamente útil.

Facebook, una red social utilizada por más de mil millones de personas al mes, dispone de los datos que el usuario deposita voluntariamente en ella, pero también hace inferencias en base a nuestras interacciones con personas e información, las comparte con terceros y elabora un perfil único que le permite determinar qué aparece en nuestro muro, tanto por parte de nuestros amigos como de anunciantes. Todo me gusta o registro a través de Facebook genera información que es analizada y clasificada por algoritmos con el fin tanto de conocernos individualmente como consumidores, como de elaborar perfiles sociales destinados a agencias de publicidad. El registro continúa incluso si hemos cerrado

la página: a no ser que salgamos manualmente, las *cookies* de Facebook continuaran espiando todo lo que hacemos *online*.

Si, además, hemos instalado Facebook en nuestro teléfono móvil, junto con su aplicación de mensajería, el sistema podrá activar remotamente nuestra cámara o micro, acceder a nuestras fotografías y mensajes, etcétera, y así ir perfeccionando nuestro perfil.

El ejemplo de la navegación web es el más habitual, pero ya no el único protagonista. El mismo despliegue de conexiones no aparentes y de compraventa de datos se produce también cuando utilizamos una tarjeta de fidelización de cliente, que relaciona nuestro patrón de consumo con un nombre, dirección, a menudo unos datos bancarios y las respuestas al cuestionario que habitualmente acompañan la solicitud.

A no ser que salgamos manualmente de la página, Facebook continuarán espiando lo que hacemos.

Otro ámbito en el que la recogida de datos es cada vez más relevante es el espacio público. Nuestro incauto deambular por las calles tiene cada vez menos de anónimo, y los sensores que leen los identificadores únicos y la geolocalización de nuestros dispositivos, las cámaras termales y de video vigilancia, las redes wifi, las farolas inteligentes o los sensores de lectura automática de matrículas nos incorporan de forma rutinaria a bases de datos públicas y privadas que en algún lugar le sirven a alguien para obtener un beneficio que ni conocemos ni controlamos.

El ámbito doméstico es quizás el espacio dónde esa monitorización de nuestros movimientos y rutinas para elaborar patrones vendibles aumenta de forma más preocupante: todos los electrodomésticos inteligentes, del contador de la luz al televisor, pasando por la nevera, construyen una red de extracción de datos que

quiere perfeccionar la imagen de quiénes somos, qué queremos o qué podemos querer. El reto es ser capaz de adelantarse a nuestras necesidades para tentarnos a adquirir productos o servicios que aún no sabemos que deseamos. Pagamos, pues, dos veces: cuando adquirimos el electrodoméstico o abonamos el recibo de la luz, en euros, y cada vez que le proporcionamos información, con datos personales.

Hay empresas que han empezado a explorar la posibilidad de convertirse en *data brokers*de los ciudadanos, una especie de corredores de datos que gestionarían nuestra información devolviéndonos una parte del beneficio generado por ella. Que nadie espere hacerse rico: de momento las empresas que intentan abrirse camino en este turbio mundo no dan más que unos cuantos euros al mes a cambio de información tan sensible como datos médicos o bancarios. De momento, el verdadero dinero no se encuentra en la relación entre ciudadanos y servicios que recogen datos. La economía de los datos es aún poco más que una promesa, de la que hasta ahora se benefician muy pocos actores (Facebook o Tuenti, Google,Foursquare, YouTube, etc.), y más por la fiebre inversora que por la cuenta de resultados. Al albor de esta promesa de negocio, eso sí, proliferan los corredores de datos dedicados al cruce de diferentes bases para aumentar el precio de venta de los perfiles generados a partir del cruce de información de actividad *online* y *offline*: los informes médicos, por ejemplo, pueden añadir mucho valor a un historial de búsqueda en Internet.

Hay empresas que ya exploran la posibilidad de convertirse en 'brokers' de datos de los ciudadanos

A algunos este escenario no les genera ninguna inquietud. Pagar con información propia abre también la puerta a la promesa de servicios personalizados y atención individualizada. Sin embargo, los corredores de datos no se limitan a cruzar detalles de lo que compramos, con quién interactuamos y qué nos gusta. Este comercio incluye también, y cada vez más, historiales médicos, datos fiscales y de renta o datos bancarios. El tipo de información que puede determinar si se nos

concede un crédito, si se nos ofrece un seguro médico más o menos caro o si conseguimos un trabajo. De repente, el precio pagado con información personal emerge como algo totalmente desproporcionado e incontrolable.

Al aceptar nos convertirnos en el producto, pues conviene no olvidar que aceptamos también que se nos pueda acabar apartando del juego, escondidos o ignorados porque nuestro perfil no aporta la solvencia, salud u obediencia esperada. (Tomado de *El País*)

Gemma Galdon Clavell**, doctora en políticas públicas y directora de investigación en Eticas Research and Consulting. visto en **La Pupila Insomne

---

Fuente: El Ciudadano