GETTY IMAGES

PRIVACIDAD

Intimidad, el paraíso perdido

Gobiernos, operadoras y empresas saben cada vez más de nosotros, la pérdida de privacidad parece imparable. Pero algunos movimientos arrojan una luz de esperanza.

JUAN MANUEL GARCÍA CAMPOS

HUBO UN TIEMPO no tan lejano en el que la mayoría de la gente no acostumbraba a colocar un cartel en la puerta de su casa para comunicar a quien quisiera darse por enterado que se iba de vacaciones a una playa al otro extremo del país. A nadie se le ocurría actualizar públicamente y a diario la información sobre sus planes personales. Al contrario, lo normal era pedir a familiares o amigos íntimos que recogiesen nuestro correo mientras veraneábamos lejos del domicilio. Que las cartas rebosasen el buzón se consideraba una imprudencia porque daba pistas a los cacos.

Hoy en día, los amigos de los amigos de nuestros hijos tienen acceso a través de las redes sociales a fotografías que nos etiquetan y geolocalizan en un chiringuito situado a 500 kilómetros de nuestro hogar. A menudo, estas imágenes vienen acompañadas de información adicional: "¡El viernes se acaba lo bueno!". Hemos abierto las puertas de nuestra esfera privada a desconocidos.

Los dispositivos electrónicos que hemos incorporado a nuestra vida cotidiana han modificado nuestra mentalidad y nuestros hábitos. Compramos comida o ropa por internet, a través del ordenador, la tableta o el *smartphone*, y aceptamos –ya sea por desconocimiento o por indiferencia– ser identificados en cada transacción.

Cuando vamos a un supermercado o a la mercería nadie nos pide el DNI a la hora de pagar, ni siquiera si usamos la tarjeta de crédito. En cambio, cada vez que operamos por internet, todas las compañías involucradas en el proceso de venta –el buscador o la red social que nos ha dirigido a la tienda on line; el distribuidor y el fabricante del producto que compramos, y los anunciantes que se publicitan en estas webs– pueden saber quiénes somos, dónde estamos en el momento en que nos conectamos a su servicio, cuál es la dirección de nuestro domicilio y en qué entidad depositamos nuestro dinero. Y si se lo proponen, podrían averiguar también cuál es la marca y el sabor del yogur favorito de nuestro hijo o a quién votamos en las últimas elecciones.

En el 2015 salieron a la luz pública varios sucesos que nos ponen sobre aviso de las consecuencias que pueden tener los descuidos que cometemos en nuestra actividad on line y la desprotección de los canales digitales en los que nos relacionamos con conocidos y extraños. Entre los casos que más trascendieron está el de la web de citas Ashley Madison, una plataforma que supuestamente ponía un especial énfasis en la privacidad de sus usuarios –al estar dirigida específicamente a personas que pretenden ser infieles a su pareja– y que sin embargo no pudo impedir que se filtraran los datos personales de más de 37 millones de clientes; o el del futbolista del Real Madrid implicado por presunta complicidad en el chantaje a un compañero de selección por un vídeo sexual que cayó en manos de un delincuente común (no un experto pirata informático); o el de la australiana que publicó en su muro de Facebook una fotografía en la que aparecía exultante, sujetando una apuesta ganadora, y se encontró con que alguien de su red de contactos imprimió el código de barras del boleto y cobró el premio en su lugar.

En el origen de todos estos casos –y de miles de otros que no se divulgan en los medios por temor o por vergüenza de los afectados– hay un par de comunes denominadores: no tenemos conciencia del valor que tienen nuestros datos personales y no hemos aprendido a percibir el riesgo de interactuar con los objetos conectados a la red.

Pero ya empieza a ser urgente un cambio de chip, porque dentro de muy poco prácticamente todas las máquinas que están a nuestro alrededor estarán conectadas a internet: el televisor, la nevera, el ▸

horno, el coche, la cámara de vigilancia de nuestro bebé, etcétera. Y lo que no son máquinas –o no lo parecen, como la muñeca habladora que dejaron los Reyes Magos o la pulsera y las zapatillas que usamos para hacer deporte–, también. Es lo que se conoce como el internet de las cosas. En lo que atañe a la privacidad, la cuestión de fondo es que cuando los aparatos que nos rodean están interconectados, nuestros datos personales también suelen estarlo.

Por otra parte, sectores como el de los fabricantes de juguetes no son industrias tecnológicas. Su objetivo es que sus productos funcionen y se vendan. Si para que se vendan más conviene que estén conectados a internet, así se hará. Ya se está haciendo. Pero es probable que en este proceso se dejen puertas entreabiertas, porque no son expertos en la producción de objetos conectados y porque la protección de nuestros datos no es un elemento directo de su negocio. Ahí está la reciente polémica con Hello Barbie, una muñeca de Mattel que integra un programa de aprendizaje automático que le permite no sólo repetir unas frases pregrabadas, sino también almacenar (en los servidores de Mattel) las conversaciones que tiene con sus pequeñas propietarias, con el fin –sostienen en la compañía– de desarrollar habilidades conversacionales. Un experto en seguridad hackeó el sistema y a través de las conversaciones grabadas tuvo conocimiento de detalles privados de la familia: "Tuve acceso a información que nunca hubiera tenido que obtener", aseguró el investigador.

El internet de las cosas supone una amenaza adicional, y no menor, para la intimidad de los usuarios

Una máxima de los críticos es que "cuando un servicio es gratis, el producto eres tú"

Algunas iniciativas e instituciones parecen anticipar un cierto cambio de tendencia en la pérdida de privacidad

Para Bosco Espinosa, portavoz en España de la empresa de ciberseguridad Kaspersky Lab, la clave se halla en la concienciación: "El mundo cibernético nos facilita la vida, para lo bueno y para lo malo. Nos permite formas de comunicación que hasta hace poco eran impensables, pero también favorece el abuso. Lo esencial es entender que lo que hacemos en el ciberespacio nos puede afectar en la vida real".

Este aprendizaje es especialmente importante para los menores. Pero nadie les está enseñando las normas de uso de las redes sociales. Tampoco les estamos advirtiendo que su huella digital perdurará y que eso les puede afectar en el futuro. O en el presente. Casi todos tienen acceso a Facebook y WhatsApp antes de los 13 años, y muchos se están acostumbrando a convivir con actitudes delictivas: "El *ciberbullying* es más peligroso que el *bullying*, porque es más fácil atreverse a hostigar a un menor delante de una pantalla que en la escuela o en la calle, donde terceras personas pueden afear la conducta de los acosadores", reflexiona Espinosa. Kaspersky está llevando a cabo el proyecto Familia Segura, con el que pretende concienciar a padres e hijos de los riesgos que puede conllevar el uso imprudente de internet. "Muchos padres nos dicen: mi hijo no hace esto ni lo otro. Y tal vez sea así, pero igualmente pueden ser el objetivo de ataques".

En realidad, todos estamos expuestos. Una de las tendencias que señalan todos los expertos en seguridad informática es el *ransomware*, un tipo de ataque que bloquea dispositivos ajenos de forma remota y encripta los archivos, de modo que el usuario pierde el control de su información y de los datos que tiene almacenados. A cambio de quitar esta restricción, el ciberdelincuente pide un rescate. Normalmente, dinero. Algunos usuarios de Ashley Madison sufrieron este tipo de extorsión: "Cada vez se conocen más casos de gente que no guarda en ningún otro sitio las fotos de sus hijos o documentos de trabajo y que está dispuesta a ceder a pequeños chan- ▸

tajes, como pagar 50 euros, con tal de recuperarlos", sostiene el experto.

En el mejor de los casos, estas brechas de seguridad sirven para que nuestra información personal se convierta en metadatos que serán explotados por las empresas cuyo negocio consiste en segmentar los datos. Es decir, en transformar la información personal en perfiles de consumidor. ¿Quiénes compran estos informes? Otras empresas a las que les interesa conocer mejor a sus potenciales clientes. El resultado son expedientes que clasifican a las personas en grupos como "joven vegetariana con altos ingresos" o "enfermo de diabetes con deudas".

Las corporaciones empresariales aducen que el objetivo del tratamiento masivo de nuestros datos personales es mejorar nuestras condiciones de vida. Y es cierto que, en general, este proceso facilitará la gestión de nuestras actividades. Como consumidores, recibiremos ofertas de productos adaptados a nuestros gustos, incluso a través de aplicaciones que vendrán preinstaladas en nuestros frigoríficos; como pacientes, podremos medir nuestros niveles de glucosa simplemente poniendo nuestro pulgar en el sensor táctil del móvil; como usuarios de la vía pública, el navegador de nuestros coches nos dirigirá automáticamente a los huecos libres para aparcar. Podremos incluso controlar el termostato y el microondas de manera remota a través del *smartphone*, de modo que cuando entremos por la puerta de casa nos encontremos una temperatura agradable y la comida preparada.

INFANCIA
Algunos juguetes tienen la capacidad de almacenar conversaciones familiares, pero pueden ser hackeados

SANIDAD
Numerosas apps nos ayudan a tener una vida más saludable, pero ¿nuestra información es segura?

MENSAJERÍA
¿El futuro pasa por sistemas de mensajería capaces de cifrar el contenido, como los que ya están empezando a proliferar

La constatación de la vigilancia masiva a la que estamos sometidos, cuestión que pasó al primer plano del interés ciudadano con las revelaciones de Julian Assange (Wikileaks) y Edward Snowden (soplón de las actividades de espionaje de la NSA), ha provocado reacciones contrapuestas. Por una parte, hay personas que están dispuestas a renunciar a su privacidad, o a buena parte de ella, como contraprestación de los servicios que disfrutan. Google, Facebook y WhatsApp nos hacen la vida más fácil y divertida. Y son gratis. Y en cualquier caso, aducen, "no tengo nada que esconder". Ante esta postura cabría objetar una frase muy recurrida por los expertos en marketing digital: "Cuando un servicio es gratuito, el producto eres tú". También hay quienes compran el principal motivo que aducen los gobiernos para controlar la red: la monitorización como garantía de seguridad ante amenazas como el terrorismo o la pederastia. Otros dibujan un panorama apocalíptico: un mundo vigilado que ha superado con creces la ficción distópica descrita por George Orwell en su novela *1984* o etapas oscuras de la historia, como la RDA de la Stasi.

El analista y consultor de nuevas tecnologías Pablo Iglesias es moderadamente optimista respecto al futuro de la privacidad: "Los gigantes de internet han empezado a dar pasos en favor de la privacidad de sus usuarios". Y apunta algunas tendencias positivas: "WhatsApp empezó hace más de un año a cifrar los mensajes que pasan por sus servidores para protegerlos de los intrusos; casi todos los servicios masivos de comercio electrónico han apostado por los protocolos de comunicación más seguros (HTTPS); las empresas están poniendo más interés en los procesos de anonimización de bases de datos, de tal modo que la información personal que se recaba de los usuarios no permite identificarlos, y algunos gigantes de internet están instalando sus centros de datos en Europa, ya que en EE.UU. están obligados a ceder los datos al gobierno, mientras que en la UE la legislación no es tan restrictiva". Y quien de todos modos no acepte este trato tiene cada vez más alternativas, como la guía práctica que ofrece Mozilla para navegar de incógnito a través de Firefox o la red de anonimato Tor, que mantiene en secreto la dirección IP (la que identifica el dispositivo de conexión a internet) y la información que viaja por ella.

En cuanto a la mensajería instantánea, están ganando terreno los sistemas que utilizan la comunicación efímera. Como Snapchat, una aplicación para enviar mensajes y archivos que se autodestruyen a los pocos segundos de haber sido vistos por el destinatario. Los jóvenes demandan este tipo de servicios. A los menos jóvenes estas herramientas les evocarán los tiempos del *Superagente 86*, que trabajaba para la agencia de espías CONTROL y combatía a KAOS, "la organización del mal". En nuestros días, el caos del ciberespacio también se combate con el control. Del uso responsable de nuestros gadgets (nombre de otro inspector que usaba la comunicación efímera) dependerá que sean tan útiles para nuestros intereses como el *zapatófono* de Maxwell Smart. ■