es

Escuela Social de Tudela y la Ribera

CURSO 2015– 2016

TEMA GENERAL

"NUEVOS DESAFÍOS EN UN MUNDO GLOBALIZADO"

5

Febrero/ 2016	TEMA	PONENTE
Martes 9: Ponencia	**"LA MANIPULACIÓN DE LA PRIVACIDAD EN INTERNET."**	**Ana Gómez Pérez Nievas** *Periodista, responsable de Medios de Comunicación de Amnistía Internacional en España*

ORGANIZA

Fundación Acción Solidaria
www.fundaciónacciónsolidaria.es
Facebook: www.facebook.com/Escuela-Socialde-Tudela-y-la-Ribera-1527087614194115
Email: fas.tudela@gmail.com
Palacio Decanal – Plaza San Jaime, 2
31500 – Tudela

De 8,00 a 9,30 de la tarde

¿Qué hacen con nuestros datos en internet?

La información personal se ha convertido en un producto más de compraventa. Deambular por los mundos real y virtual tiene cada vez menos de anónimo.

Por Gemma Galdon Clavell

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.

Sigue.../...

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.

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 estè 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.

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.

Gemma Galdon Clavell, doctora en políticas públicas y directora de investigación en Eticas Research and Consulting.

- ***Consulte otros temas en el suplemento IDEAS***

Sigue.../...

Más información

- ***La casa en el árbol***
- ***El efecto Snowden***
- ***¿A alguien le importa la privacidad?***
- ***La batalla global por los datos***

Una vida vigilada

- Tecnología y dispositivos que producen o almacenan datos de nuestra actividad cotidiana:
- **1/6/14**. Videovigilancia: las imágenes pueden ser interceptadas.
- **2.** Contadores de luz y termostatos: dan información de hábitos.
- **3 /4.** Televisores inteligentes y consolas: incorporan cámaras y micrófonos.
- **5.** Controles biométricos de entrada y salida.
- **7.** Monitorización remota en el trabajo: capturas de pantalla del trabajador para medir la productividad.
- **8.** Bases de datos personales: pueden contener datos fiscales y de salud de los clientes.
- **9.** Sensores de conteo de personas: monitarizan el flujo de compradores y los tiempos de compra.
- **10.** Tarjetas de fidelización: a cambio de descuentos, crean perfiles del comprador.
- **11.** Ibeacons: envían ofertas a móviles cercanos.
- **12.** Wifi gratuito: se puede ofrecer a cambio de acceso al perfil de Facebook.
- **13.** Abonos de transporte público: tarjetas recargables que producen datos de desplazamientos.
- **14.** Redes de bicicletas públicas: registro de trayectos.
- **15.** Coches: hay sistemas para registrar las matrículas.
- **16.** Telefonía móvil: permite geolocalizar.
- **17.** Cámaras térmicas y sensores sonoros: miden flujo de peatones y niveles de ruido.
- **18.** Mobiliario urbano que detecta presencia de peatones.
- **19.** Sistemas de párking: el pago con tarjeta de plazas azules y verdes genera datos del usuario.

¿Te vas de vacaciones? Cuidado con conectarte a redes de WiFi abiertas

"Engancharse a señales desconocidas pone en riesgo la privacidad de tus datos"

Laura Delle Femmine - Madrid

Estás de vacaciones en el extranjero y llevas días sin poderte conectar a ***Internet***. De repente, tu ***smartphone*** te avisa de que hay una ***red WiFi*** a tu alcance, que tiene el mismo nombre del bar donde estás desayunando. ¡Y no pide contraseña! ¿Qué suele ocurrir? te conectas y piensas que has sido afortunado. Cuidado: quizá has picado y te acabas de convertir en la víctima perfecta de alguien dispuesto a robarte claves, números de cuenta o fotos personales.

"El problema es que no sabes de quién es la red. Podría ser maliciosa o ***hackeada***", comenta Luis Corrons, director técnico en la ***empresa de antivirus Panda Security***. El experto en seguridad informática alerta de la necesidad de tomar precauciones antes de ponerte a navegar. Pero, ¿cuáles son los riesgos que corremos y cómo podemos defendernos de ellos?

¿Qué riesgos corremos?

Más del 73% de los usuarios utiliza redes WiFi públicas gratuitas, de acuerdo con la última encuesta de ***Kaspersky Lab*** sobre *Hábitos de Seguridad Multidispositivo en España*. Hasta aquí comprensible. Lo preocupante es que un 40% de ellos comparte datos sensibles, personales y financieros, a través de este tipo de señales.

"Por pura inercia o vicio se hacen consultas de datos personales por conexión inalámbrica", asegura Marcos Jimena, especialista en *entreprise networking* en ***Cisco Systems***. "El WiFi se usa cada vez más, y por estadística siempre habrá alguien que caiga", comenta. Los riesgos son múltiples: desde el robo de datos y credenciales hasta la infección de los dispositivos o la suplantación de identidad.

Las señales abiertas [que no piden ni usuario ni contraseña] son las más vulnerables. Un ***pirata informático*** que está conectado a tu misma red tendría muy pocos problemas para "usurpar, hacer trazabilidad de tus datos o meterse en tu dispositivo", detalla Jimena. ¿Esto significa que si nos conectamos a una red protegida estamos a salvo? Tampoco. "La identificación no garantiza que la conexión esté bien cifrada", argumenta el experto de Cisco.

Alguien podría, incluso, haber manipulado el *router* del establecimiento o creado una señal WiFi paralela —práctica conocida como *wi-phishing*— con el mismo nombre de la red de la cafetería, tienda u hotel a la que nos vayamos a conectar. "En este caso te estás enganchando directamente al punto de acceso de un *hacker*", advierte Jimena. Uno de los ataques más típicos es redireccionar la navegación del usuario hacia páginas ficticias, sobre todo *webs* fraudulentas de bancos *online* o de correo electrónico. Si picamos, estaremos entregando nuestro número pin directamente al ciberdelincuente.

Otro riesgo es que nuestros dispositivos acaben siendo infectados. Y esto no vale solo para los ordenadores: cada mes se generan 20.500 nuevas muestras de *malwares* para móviles y tabletas, de acuerdo con Kaspersky Lab. Un dato importante, si consideramos que, en 2014, ***el 77% de los usuarios se conectó a Internet a través de su*** *smartphone*.

¿Cómo podemos defendernos?

"Nada es seguro al 100%", mantiene Marcos Gómez, subdirector de operaciones del ***Instituto Nacional de Ciberseguridad (INCIBE)***. Existen, sin embargo, algunas precauciones que, aunque no anulen todos los riesgos, sí reducen las probabilidades de sufrir ataques perpetrados por *ciberdelincuentes*. Aquí están algunas de ellas.

1. Verifica que la red WiFi no sea falsa. "Si hay dos redes con nombres muy similares debemos de sospechar", añade Gómez antes de hacer un ejemplo: "Estamos en el Café Paco y algún malintencionado crea una red bajo el nombre *Paco Café*. Así que tendemos dos redes: *Café Paco*, que es la buena, y *Paco Café*. El ciberdelincuente lo hace para que te confundas y te conectes a su red".

Sigue.../...

Por esto es recomendable que comprobemos siempre con el local con los propietarios o empleados el nombre de su punto de acceso WiFi.

2. Mantén el dispositivo siempre actualizado. ¿Cuántas veces has pospuesto la actualización de tu dispositivo? Aunque sea molesto esperar a que el aparato se reinicie, no es un "capricho del dispositivo", bromea Gómez: "Corrige problemas de funcionalidad, como agujeros de seguridad eventuales".

3. Borra el historial de redes almacenadas y apaga el WiFi. Tu dispositivo memoriza todas las redes a las que te has conectado, incluso las que usaste solo una vez. Bórralas todas y mantén solo las de confianza, como las de casa o del trabajo. También procura desconectar el sistema WiFi si no lo estás usando. Con estas pequeñas precauciones evitarás caer en las garras de un *ciberdelincuente* que esté barajando suplantar las redes favoritas de tu dispositivo.

4. Configura una red VPN. Una VPN (*Virtual Private Network*) es un servicio que permite realizar una navegación segura, por ejemplo para acceder a la información corporativa desde un lugar diferente del trabajo, aunque se puede usar también para saltarse la censura aplicada en algunos países o acceder a contenidos disponibles solo en ciertos lugares. "Es como si todas las comunicaciones estuvieran dentro de un túnel, lo que hace que todo el tráfico que sale de nuestro dispositivo esté cifrado", explica Luis Corrons de Panda Security. Esto es así porque el dispositivo se conecta a un servidor externo y es como si no se utilizara la red a la que el usuario está conectado.

5. Averigua si las páginas están cifradas. Una página está cifrada cuando aparece, al principio de la barra de direcciones, el dibujo de un candado seguido por las letras ***https***. Si pinchamos en el simbolito, aparecerán las especificaciones de la conexión, donde podremos averiguar que el certificado es válido y la página original. "Hoy en día la mayoría de redes sociales y correos electrónicos están cifradas", comenta Corrons. Lo mismo pasa con los mensajes de Whatsapp. También existen complementos, como HTTPS Everywhere de ***Electronic Frontier Foundation***, que encriptan la información que estamos manejando a través del navegador.

6. Cuidado con las sincronizaciones. Cuando te conectas a una red abierta, es mejor desactivar las sincronizaciones automáticas que siguen funcionando en segundo plano enviando y recibiendo datos. Gómez advierte de que también existen virus que están diseñados para entrar en el móvil y utilizarlo como vehículo para infectar el ordenador cuando lo conectemos. "Antes de sincronizar, habría que hacer un escaneo con una herramienta adecuada para ver si detectamos algo raro, y en ese caso limpiar el dispositivo antes de sincronizarlo", recomienda.

7. No mantengas sesiones demasiado largas. Si te conectas a una red WiFi que no conoces, no la uses durante horas como si estuvieras en tu casa, sobre todo si estás manejando información sensible.

Existen otras precauciones para reducir la probabilidad de sufrir un ataque, como instalar antivirus o realizar navegaciones anónimas. Sin embargo, recordando que la seguridad al 100% no existe, quizá el mejor consejo es tener sentido común: evita compartir datos sensibles, como las claves de tu banca *online*, el número de tarjeta de crédito, fotografías personales o los datos de tu correo electrónico cuando estés navegando a través de una red desconocida.

Más información

- ***Así pueden 'hackearte' cualquier aparato conectado a Internet***
- ***"Cada vez resulta más fácil hacerse 'hacker"***
- ***AENA dará wifi gratis sin límite en todos los aeropuertos españoles***
- ***Este es el aspecto que tiene tu WiFi***
- ***'Hackear' tu Facebook solo cuesta 91 euros y bloquear un sitio web, 15***
- ***Robar privacidad***
- ***Amenaza en la red***
- ***La pesadilla de los virus informáticos que atacan las lavadoras***

Internet está cada vez más vigilado

Freedom House alerta de la consolidación de las restricciones a la privacidad en la Red

Por María Sosa Troya - Madrid

La libertad en Internet se ha reducido por quinto año consecutivo. Se han consolidado las restricciones a los derechos de los internautas y la vigilancia a los usuarios se ha expandido. Estas son algunas conclusiones del informe sobre la libertad en la Red que este miércoles publica la organización independiente ***Freedom House***, que ha analizado la situación en 65 países —que acogen al 88% de los usuarios mundiales de Internet—. El estudio indica que cada vez más Gobiernos tratan de censurar información de interés general y presionan al sector privado para que retire los contenidos que les resultan molestos.

Más de 3.000 millones de personas navegan por Internet. Según las estimaciones de Freedom House, el 61% de ellas vive en países en los que las críticas al Gobierno, al Ejército o a las familias que están en el poder han sido objeto de censura. El informe, titulado *Libertad en Internet 2015*, sostiene que se ha producido una escalada en los arrestos y la intimidación a los usuarios. En 40 de los 65 países analizados el año pasado han sido dictadas penas de cárcel por haber compartido en contenidos a través de las redes sociales. En siete de ellos, las condenas han sido de siete años o más. En China, un tribunal sentenció al académico uigur Ilhan Tohti a cadena perpetua por "fomentar el separatismo" a través de una página web.

La organización ha realizado el estudio entre el 1 de junio de 2014 y el 31 de mayo de 2015. Su clasificación se basa en tres parámetros: los obstáculos para el acceso a Internet; los límites impuestos a los contenidos, y las violaciones de los derechos de los usuarios, incluyendo la vigilancia, la persecución legal, acoso o ataques a los internautas. Así, otorgan una puntuación a los 65 países analizados y los dividen en tres categorías: libres (18 países, entre los que están Estonia, Canadá, Alemania o Australia), parcialmente libres (28, entre los que se encuentran Turquía, México, Colombia o India) y no libres (19, entre los que se sitúan Cuba, Siria, Irán o Etiopía). Islandia es el Estado que mejor nota obtiene, frente a China, con la peor. España no ha sido evaluada.

"En muchos sentidos, el pasado año ha sido de consolidación y adaptación de las restricciones en Internet, en vez de un dramático deterioro [en el grado de libertad en la Red]. Los Gobiernos que ya habían expandido su arsenal de herramientas para controlar el entorno digital ahora están reforzando la aplicación de estos métodos", se explica en el informe. Según el estudio, los países que han experimentado una mayor caída han sido Libia —en donde se ha incrementado la violencia en contra de blogueros y se han registrado casos de censura política, así como una subida de los precios de Internet—, Ucrania —con persecuciones debido a críticas vertidas contra el Gobierno de Kiev y el aumento de la violencia de los separatistas prorrusos contra los usuarios proucranios— y Francia —que, a raíz de los ***atentados de París***, aprobó una legislación restrictiva en la Red.

La vigilancia ha ido en aumento a nivel mundial. Esta es una de las principales tendencias detectadas por Freedom House. En 14 países —también democráticos, como Francia o Australia— ***se han aprobado nuevas medidas autorizando estas prácticas***, "impulsados en parte por la preocupación por el terrorismo y por la expansión del Estado Islámico". Ciberactivistas, compañías tecnológicas y organismos internacionales han criticado las leyes que obligan a la retención indiscriminada de los llamados metadatos por considerar que violan la integridad, seguridad y la privacidad de los sistemas de comunicación.

Sigue.../...

Otra conclusión a la que llega Freedom House es el cambio de tendencia a la hora de censurar contenido en Internet. Los internautas están cada vez más preparados para esquivar esa censura, por lo que los Gobiernos optan por solicitar tanto a usuarios como al sector privado la retirada de contenidos que les resultan molestos. Así, conscientes de que es posible saltarse los bloqueos que se impongan, las autoridades presionan para exigir la retirada de la información que consideran ofensiva. En el mejor de los casos, apoyándose en la ley. En los peores, incluso recurriendo a la intimidación y a la tortura. Según el informe, en Bahréin la cuenta satírica en Twitter @Takrooz contaba con unos 100.000 tuits. Fueron borrados todos excepto uno: "Me torturaron en prisión".

Además, se ha reducido la posibilidad de protección en la Red, pues los Gobiernos han dado pasos hacia la prohibición de la encriptación y el anonimato, fundamentales en el caso de periodistas y activistas de derechos humanos, que se sirven de estas herramientas para proteger su libertad de expresión.

El estudio también recoge avances. Freedom House expone que 15 países han registrado mejorías este último año. Los principales logros, indica el informe, se deben a cambios legislativos o decisiones judiciales. Y concluye: "El activismo digital ha sido y sigue siendo el principal promotor del cambio alrededor del mundo, particularmente en sociedades que carecen de derechos políticos y libertad de prensa".

- ***GRÁFICO Libertad en Internet 2015***

  http://elpais.com/elpais/2015/10/27/media/1445965142_005567.html

¿Qué dice la sentencia del Tribunal de la UE sobre protección de datos?

La Corte considera que EE UU no es un país seguro para el envío de datos de los ciudadanos.

Por Nicolas Bouvy (EFE)

Los Estados miembros de UE podrán a partir de ahora bloquear el envío de datos personales a EE UU, según una sentencia del Tribunal de Justicia de la UE publicada esta mañana sobre la que no cabe recurso. El fallo otorga a las agencias nacionales de protección de datos la posibilidad de parar las transferencias de datos de ciudadanos europeos a terceros países (incluido EE UU) si consideran que la empresa —o territorio— a la que se destinan no es fiable. Esto quiere decir que el criterio de las agencias prevalecerá sobre el de la Comisión Europea, que desde hace 15 años considera EE UU un puerto seguro.

¿Qué dice la sentencia?

La sentencia, de tres páginas, establece que tanto en la ley como en la práctica "EE UU no garantizaba una protección suficiente de los datos transferidos a ese país" y solicita a la Comisión que invalide la norma según la cual el territorio era considerado seguro para la intimidad de los ciudadanos europeos desde hace 15 años.

La Justicia europea reprocha al Ejecutivo comunitario que no haya comprobado si EE UU garantiza un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en la UE y que se haya limitado simplemente a "analizar".

¿Por qué se ha pronunciado el Tribunal de Luxemburgo?

Un ciudadano austriaco de 27 años, Max Schrems, interpuso una denuncia en Irlanda contra Facebook —país donde la compañía tecnológica estadounidense tiene su filial europea—, porque consideraba que la empresa no garantizaba la seguridad de sus datos. Schrems presentó su denuncia tras el estallido del caso de espionaje de la NSA, en 2013, cuando el exanalista de la agencia norteamericana, Edward Snowden —ahora asilado en Moscú—, reveló que la inteligencia estadounidense tenía acceso a los datos de esta y de otras compañías. La Corte irlandesa remitió la consulta al Tribunal de Justicia de la UE, que ha fallado ahora a favor de Schrems.

¿Por qué las compañías transfieren los datos de los usuarios?

Los datos de los usuarios recogidos por las empresas en la web tienen que ser almacenados en servidores. Todo lo que compartimos o escribimos en Internet —desde las fotos personales hasta los datos de la tarjeta de crédito— se almacena en ***servidores,*** que en muchos casos se hallan en EE UU.

¿Qué es el acuerdo 'safe harbour' (puerto seguro)?

Se trata de un pacto entre EE UU y la Comisión Europea que, hasta el momento, permitía a las empresas transferir datos a través del Atlántico. La condición que la UE ponía para esa transferencia era que se realizara con países que respetasen el marco legal europeo de protección de la privacidad, como, por ejemplo, notificar al cliente cuando se utilizan informaciones personales y con qué finalidades.

¿Cuántas empresas se verán afectadas?

Hay más de 4.400 empresas que dependen de este acuerdo. Estas empresas tendrán que reestructurar sus negocios para evitar una infracción de la normativa comunitaria. Las empresas más pequeñas son las que más sufrirán la interrupción de este pacto en Europa.

¿Qué pasará ahora?

Todo está realmente en el aire. Bruselas y Washington han intentado durante meses lograr un nuevo acuerdo sobre el asunto. Sin embargo, después de la resolución del Tribunal de Luxemburgo, la Comisión Europea tendrá menos capacidad de maniobra, los eurodiputados controlarán su labor, y es muy probable que las negociaciones para alcanzar un nuevo acuerdo duren varios meses.

Lo saben todo sobre usted

Incontables cámaras de vigilancia escrutan sus movimientos.
Ordenadores de capacidades descomunales rastrean sus huellas en la Red
Entramos en un universo controlado por 'hackers', Gobiernos, empresas y traficantes de datos.

FOTOGALERÍA Los datos están en el ciberespacio

Por Luis Miguel Ariza

Es española, de mediana edad. Se levanta a las siete de la mañana. Activa su teléfono móvil para comprobar el correo electrónico. Las luces de un servidor parpadean a kilómetros de su casa. Mientras lee las noticias en su tableta, navega por Internet y apura su taza de café, otro disco duro registra cada clic en sus tripas informáticas. Los algoritmos de **Google** –cuyo navegador es el más usado en el mundo– registran cada migaja de información en sus máquinas: qué páginas ha visto o leído y a qué hora exacta, qué videos ha visionado, dónde se encuentra la usuaria. Nuestra protagonista tiene una presentación en la oficina y repasa el último borrador en su flamante iPhone. Una copia se almacena automáticamente en la nube. La nube no es algo etéreo: miles y miles de **servidores** se apilan en armarios descomunales. Discos duros refrigerados dibujan pasillos larguísimos en funcionamiento ininterrumpido dentro de búnkeres a prueba de terremotos y envueltos en un monocorde ruido que rompe el silencio.

Más rutina diaria. Subir una foto en Facebook. Responder a un tuit. Ir en el coche al trabajo. Cerrar una reserva en el restaurante mediante una aplicación y enviar un mensaje para cuadrar la cita con otros comensales. El GPS del móvil rastrea la localización cada segundo. Otra aplicación hace que un servidor conozca los teléfonos móviles de todos sus contactos de chat. El móvil escupe sugerencias sobre otras personas a las que conocer. Un poco de deporte antes de ir al trabajo permitirá que la cinta wifi atada a la muñeca transmita al móvil el número de pasos, pulsaciones, el ritmo cardiaco y la temperatura de su piel, memorizados en otra máquina. Su teléfono sabe dónde está con un margen de error de menos de un metro. Lo mismo ocurre con los comensales del almuerzo.

El mundo totalitario de Winston Smith, protagonista de ***1984***, se caracterizaba por una lucha por proteger la privacidad. Las violaciones personales eran constantes. La telepantalla vigilaba sus movimientos durante las 24 horas. Uno no estaba seguro de si lo escuchaban y debía actuar como si lo hicieran. Cualquiera podría ser el observador que lo llevara a la cárcel, al dolor o a la muerte en nombre del partido. No bastaba con fingir. Había que actuar de manera convincente para impedir que los ojos te descubrieran, reaccionar como los demás. La vigilancia era tan intensa que los padres temían que sus hijos les delatasen. Cualquier desviación de la rutina, como llegar al trabajo con los dedos un poco manchados de tinta, despertaba suspicacias acerca de si ese fulano estaba escribiendo, qué hacía y por qué.

Los servidores conocen hasta a la persona con la que duermes"

El salto hasta 2015 desde la distopía de la sociedad de *1984*, de George Orwell, repleta de recursos increíbles para la vigilancia, nos zambulle en un mundo extraño y contradictorio. Los flujos de información van y vienen, invisibles por el aire, y quedan almacenados en cascadas de servidores.

"Hablan sobre los lugares que visitas, con quién te ves con más frecuencia y durante cuánto tiempo, tus gustos, hasta con quién duermes", asegura Bruce Schneier, jefe de tecnología de la compañía Resilient Systems, en su libro ***Data Goliath: The Hidden Battles to Collect your Data and Control your World*** **(Norton, 2015).** Los *smartphones* actuales no funcionan a menos que la compañía sepa dónde se encuentra el usuario. Y los sistemas operativos de los ordenadores se parecen cada vez más al de los móviles.

En realidad, ya son lo mismo. En los mejores tiempos de la República Democrática Alemana, la Stasi contaba con 102.000 agentes que espiaban a una población de 17 millones, lo que significaba un espía por cada 166 ciudadanos –la cifra se reducía hasta 66 si se contaban los colaboradores–. Los teléfonos y las grabaciones eran indispensables para los chivatazos. Ahora el teléfono ha muerto.

Sigue.../...

En su lugar llevamos una máquina que nos rastrea y que lo sabe casi todo sobre nosotros. En 2016 se calcula que más de dos mil millones de personas usarán estas minicomputadoras. Aún las llamamos teléfonos, pero nunca, nunca descansan. Extraen información y la envían fuera de nuestro alcance. ***¿Es exagerado equipararlas a las telepantallas de la distopía orwelliana?*** Ricard Martínez, presidente de la Asociación Profesional Española de Privacidad, no lo duda. "La monitorización hoy día es incluso mayor que como la describió Orwell".

Vivimos en la edad de oro de la vigilancia. La compañía británica Cobham comercializa un sistema que envía una señal ciega e indetectable a un teléfono, la cual no le hace sonar y permite la localización de su dueño a menos de un metro; Defentek, con base en Panamá, asegura que posee un *software* con capacidad para detectar cualquier teléfono móvil en el mundo sin que el operador ni su dueño se enteren, y la Agencia de la Seguridad Nacional de EE UU sostiene que es capaz de rastrear móviles incluso cuando están apagados. **¿Dónde ha quedado la privacidad?**

Los gigantes que hoy dominan el mundo, Facebook, Apple, Twitter y Google, facturan miles de millones de dólares cada año y responden con páginas y páginas de farragosas explicaciones en letra pequeña escritas en lenguaje de leguleyo. Insisten en afirmar que sus compañías no venden a terceras partes la información personal del usuario, pero eso no es exactamente así. Disponen de esa información porque se la hemos dado gustosamente. Y a ciegas. En todas se especifica el consentimiento del usuario para compartirla con terceras empresas. "Proporcionamos a los anunciantes información sobre el rendimiento de sus anuncios, pero lo hacemos sin ofrecer ningún dato que te identifique personalmente", aclara por correo electrónico Anaïs Pérez Figueras, directora de comunicación de Google España y Portugal. "Podemos indicar a un anunciante cuántos usuarios han visto sus anuncios o han instalado una aplicación después de ver un anuncio concreto. También podemos ofrecerles información demográfica general, como, por ejemplo, hombres de entre 25 y 34 años que viajan". En la era digital, insiste Figueras, "no estamos perdiendo la privacidad".

En realidad, la hemos regalado a cambio de servicios que se presentan como gratuitos, pero que no lo son. "Uno de los grandes problemas de la privacidad es el usuario, que no la valora", recuerda Martínez, refiriéndose al fracaso cuando WhatsApp intentó cobrar un euro al año a los usuarios.

Escuchar la palabra "gratis" es irresistible. Estos gigantes de la Red se han convertido en los embajadores de la gratuidad. Pero nuestros datos personales significan dinero. Eli Pariser, activista de Internet, autor del superventas literario ***The Filter Bubble*** (Viking) y anterior presidente del grupo Move On, calcula en 500 dólares lo que cada usuario regala a Google cada año. Lo afirma en el documental *Terms and Condition May Apply*, del director Cullen Hoback. "Google, Facebook o Twitter no comercian con datos personales", explica Schneier por correo electrónico. "Cobran a otros por usar los datos, pero no los venden a otras compañías. Pero no estoy seguro de si esta diferencia es la que marca la diferencia". Los consumidores ordinarios hemos dejado de ser clientes para convertirnos en productos por la información que generamos. Cuanto más sepan de nosotros, más jugosos serán los beneficios en el mercado digital. ¿Quiénes se benefician y qué datos manejan exactamente?

En 2014, la Comisión Federal de Comercio de Estados Unidos (CFC) publicó un informe revelador sobre esta industria multimillonaria. Estudió nueve compañías: Acxiom, CoreLogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, RapLeaf y Recorded Future. Su negocio consiste en analizarlo todo: transacciones bancarias y compras, campañas de *marketing*, detección de fraudes, verificación de identidades digitales, publicidad en hogares, obtención de perfiles de los usuarios; nombre, edad, sexo, estado civil de los dueños de correos electrónicos e incluso historiales para predecir qué compraremos en el futuro basándose en hábitos pasados. Los servidores de Acxiom contienen información sobre 700 millones de consumidores en todo el mundo. Cada cliente estadounidense está asociado a 3.000 fragmentos de información. ID Analytics cubre 1.400 millones de transacciones comerciales. Y Recorded Future exprime la información de los usuarios al tener acceso a más de 502.591 páginas web.

Estas compañías –Data Brokers, en inglés, o agentes de datos– obtienen la información a partir de muchas fuentes: otras empresas, el Gobierno, incluyendo datos sobre quiebras bancarias, registros de garantías... pero no directamente de los propios consumidores, los cuales, en su inmensa mayoría "desconocen que están extrayendo y usando esa información", reza el estudio de la CFC.

Sigue.../...

La combinación de esta increíble cantidad de datos genera clasificaciones como "propietario de un perro", "entusiasta de actividades de invierno", si se es negro o latino con bajos ingresos, si se tiene más de 66 años, si se atesora poca educación o posesiones poco valiosas, si se vive más en el campo entre los treinta y cuarenta años con ingresos por debajo de la media, si estamos ante un "matrimonio sofisticado", si se va a ser padre por primera vez, si alguien es diabético o tiene problemas con el colesterol...

Algunas de estas compañías ofrecen a otras empresas un sistema de pago de búsqueda de personas basado precisamente en los metadatos. A partir de una dirección, teléfono, correo electrónico o un simple nombre de usuario, las compañías permiten a sus clientes utilizar estos sistemas de búsqueda para averiguar los alias, edad y fecha de nacimiento, nombre, género, números de teléfono, educación, defunciones, información sobre sus familiares, historial de empleo, número de matrimonios y divorcios, juicios, bancarrotas y acreedores, propiedades e historial de préstamos, información sobre redes sociales y nombres de usuarios, y vecinos (incluyendo si alguno se ha involucrado en casos de abuso sexual).

En el programa de televisión ***60 minutos***, de la cadena CBS, la comisionada federal de comercio Julie Brill afirmó que estas compañías elaboran "expedientes sobre personas sin que la mayoría de los investigados lo supieran. El estudio de la CFC no oculta los beneficios que los consumidores pueden disfrutar por la actividad de estas entidades: una oferta competitiva de productos más adaptados a sus gustos, o minimizar los riesgos de las compañías financieras para prevenir fraudes a la hora de otorgar créditos. Pero hay contradicciones: alguien calificado como un entusiasta de la bicicleta podría beneficiarse de cupones de descuento de un vendedor de motocicletas, pero ser interpretado como un cliente de riesgo para la compañía de seguros y sufrir discriminación por ello. Bajo el epígrafe de "Interés por ser diabético", puede conseguir ventajas en la oferta de alimentos sin azúcar y al mismo tiempo ser clasificado como una persona de alto riesgo para el seguro médico.

¿Qué son exactamente los metadatos? Si usted llama a un amigo o chatea con él, los metadatos hablan de la frecuencia con la que lo hace con esa persona, el tiempo empleado, la hora del día o el número de palabras, pero no su contenido. Los metadatos indican qué restaurantes frecuenta, lo que uno compra, las páginas web que visita, el número de correos electrónicos, la localización, los centros o tiendas a los que llamamos... Y pueden ser muy reveladores.

Un estudio de investigadores de la Universidad de Stanford recogió todos los metadatos producidos por los *smartphones* de más de quinientos voluntarios durante varios meses. Los científicos habían diseñado una aplicación que se instalaba en sus teléfonos y que enviaba el flujo de información. Se quedaron estupefactos por lo que pudieron averiguar. Uno de los participantes se comunicaba con grupos de personas que sufrían lesiones neurológicas y con un número de teléfono de un laboratorio farmacéutico especializado en medicamentos para la esclerosis múltiple; otro realizaba frecuentes llamadas a un vendedor de armas semiautomáticas, y los metadatos de otro usuario descubrieron que telefoneaba y recibía llamadas de una farmacia, un laboratorio y una línea de un centro especializado en tratar arritmias cardiacas.

En otro caso se supo que una persona cultivaba marihuana en su casa a raíz de las llamadas que hacía a un distribuidor de sistemas de cultivo hidropónico, a un cerrajero y a una tienda que dispensaba semillas de esa planta y vaporizadores. Una mujer mantuvo una larga conversación con su hermana y a los dos días realizó una serie de llamadas a un centro de planificación familiar; dos semanas después hizo otras llamadas más breves, y un mes más tarde telefoneó al mismo centro, lo que sugería que la mujer había tenido un aborto. Jonathan Mayer, uno de los autores del estudio, explicó que, por respeto a la intimidad, se confirmaron en persona solo los casos del poseedor de armas automáticas y el de quien había realizado las consultas sobre arritmias. "Fuimos capaces de identificar un número de patrones que eran muy indicativos de actividades o rasgos sensibles", comentó Mayer a *Stanford Daily*.

El diario *The New York Times* publicó al respecto una historia singular. Un padre acudió a las oficinas de Target, un centro comercial que vende prácticamente de todo, desde DVD y alimentación hasta artículos de limpieza.

El hombre se quejaba de que la compañía estaba enviando a su hija, que aún estudiaba en la escuela secundaria, publicidad y cupones descuentos para futuras madres. El padre no sabía que su hija estaba embarazada.

Sigue.../...

El matemático Andrew Pole, contratado por la empresa, había establecido un programa por el que la compra de 25 clases de productos asignaba a las mujeres una probabilidad muy alta de embarazo. Los estudios sugerían que ellas cambian rápidamente sus hábitos de compra durante el primer trimestre, al adquirir productos como vitaminas y suplementos alimenticios, jabones y lociones no perfumadas o grandes bolsas de bolas de algodón. Se trata de un filón de ventas para una compañía que pueda identificarla de antemano. El departamento de *marketing* se puso en contacto con Pole para saber si podría escribir un programa que descubriera a una mujer embarazada por el cambio de sus hábitos de compra.

Para Ricard Martínez, "las grandes corporaciones empresariales no usan los datos en sentido negativo como los Estados. Pero toman decisiones sobre nosotros sin contar con nosotros". Sugiere la visión optimista de un futuro en diez años: todo estará conectado a Internet, desde el coche hasta el horno... Se pagará todo con el móvil, que te dirá qué restaurante te va a gustar más sin importar en qué ciudad estés. "¿Qué te parecería pagar el seguro solo de las horas que conduces, que te guíen a una plaza de aparcamiento libre, o te adviertan de tu nivel de glucosa en sangre en tiempo real antes de un problema diabético? ¿Y pedirle a tu robot que te caliente la cena cuando estés a 10 minutos de casa? Todo ese universo necesita datos, perfiles, preferencias, patrones de conducta". Al mismo tiempo, recalca, es necesario defender la privacidad y encontrar un espacio de equilibrio. "Lo que está en juego es la libertad".

Todo queda grabado en las redes sociales. Cualquier cosa que hagamos llegar al ciberespacio permanecerá ahí para siempre. Los adolescentes que han nacido en la era digital están esculpiendo tuit a tuit una identidad imposible de borrar que les perseguirá toda la vida: Su pasado quedará expurgado de secretos y disponible para la visión del público. ¿Por qué? Las compañías ofrecen la posibilidad de borrar los perfiles y las fotos –hay ciertas dudas técnicas sobre si es posible borrar todo el material repicado en servidores–, pero la huella digital perdura. Los compartidos de Twitter o los *me gusta* de Facebook se multiplicarán en otros perfiles de usuarios. En sentido orwelliano, ya no es necesario vigilar a los adolescentes con una telepantalla. Una vez que entran en la tela de araña cibernética, quedan atrapados. Ellos mismos hacen el trabajo.

Las grandes corporaciones toman decisiones por nosotros sin contar con nosotros"

El primer error que cometen es mentir sobre la edad cuando se inscriben en Facebook, Twitter o Tuenti. "Muchos jóvenes no tienen conciencia de que lo que ponen en las redes va a marcar su huella digital y su identidad *online*", advierte Esther Arén Vidal, inspectora jefa y delegada provincial de participación ciudadana del Cuerpo Nacional de Policía. "Queda ahí para toda la vida. Si supieran las consecuencias de lo que cuelgan o publican, la mitad de las cosas ni las harían". Antaño, si uno tomaba fotografías, guardaba los negativos y las copias. Si se compartían con amigos, la confianza de que no serían usadas algún día de forma comprometedora dependía de unas pocas relaciones. Pero en esta era digital en la que la mayoría de los adultos nos hemos convertido en inmigrantes digitales, las nuevas generaciones utilizan las redes sociales sin haber recibido la formación necesaria ni las normas de uso. "Es como montarse en un coche y acelerar sin que nadie te explique el funcionamiento de los controles", explica Arén. Una de las primeras consecuencias de ese desconocimiento es la pérdida inmediata de la privacidad.

Esta responsable policial imparte charlas en los colegios para paliar el desinterés de las compañías de las redes sociales en explicar los peligros a los menores. Y narra situaciones antes inimaginables. Padres cuyos hijos recibían quimioterapia que contaban en sus mensajes de WhatsApp el nivel de los fármacos y la evolución de la enfermedad, y niños que al leerlos "pensaban que se iban a morir". Los mismos padres que informan en sus blogs sobre la enfermedad de sus hijos, violando la ley de protección de datos y comprometiendo la vida futura del menor al alcanzar la mayoría de edad. En otros casos, progenitores poco discretos que involucran a sus hijos mientras chatean en las redes sociales, contando chismes sobre ellos, engordando la identidad digital que les perseguirá toda su vida cuando alcancen la mayoría de edad. Casos de hijos que denuncian a sus padres por indiscretos.

En una clase de niños y niñas de 10 años, algunos levantan la mano cuando se les pregunta si tienen Facebook o Twitter. "Con 14 tienen todos, y admiten que mintieron sobre su edad para entrar en Facebook". Lo admiten ante un agente uniformado. **Sigue.../...**

Los patrones de los delitos, algunos de los cuales están explicados en el libro *Internet negro* (Temas de Hoy), de los policías Pere Cervantes y Oliver Tauste, se repiten. Una niña de 12 años empieza a sufrir acoso por mensajes de los grupos de WhatsApp; no aguanta más y se quita del grupo, pero sus compañeras se ocupan de que le lleguen los improperios. Alguien insulta. Hay una víctima y otros que consienten. "Se acostumbran a vivir con el delito y miran hacia otro lado", dice Arén, que prologó el libro de sus compañeros.

Una menor se enamora y un chico le pide fotografías, imágenes en las que se desnuda o se masturba. Cuando ella quiere dejarlo, el niño difunde el vídeo a toda la clase.

"Llevo dos años y medio viendo el mismo caso con distinto nombre y en distinto colegio", prosigue Esther Arén. "La mayoría de los delitos los cometen menores de entre 10 y 14 años, que no pueden ser imputados. La mayoría no lo denuncia y los padres no tienen conocimiento, y en el colegio suelen decir que son cosas de niños y no intentan conseguir pruebas. Es como una bomba de relojería. No se ha detectado el problema hasta que se producen intentos de suicidio por parte de los niños".

Se trata de un cepo del que es muy difícil soltarse. Si alguien decide suplantar una identidad digital, el afectado tiene que rellenar el cuestionario de la compañía de la red social, que no siempre es accesible ni fácil, llevarlo a una comisaría, denunciar la suplantación y esperar a que un juez ordene a la compañía borrar la identidad falsa. "Estamos muy poco protegidos frente a estas empresas, que muchas veces solo miran el negocio en vez de cuidar del menor y de su privacidad", asegura esta inspectora jefa de la policía. Ella admite que no existe aún un hábito de colaboración por parte de estos gigantes informáticos, cuyos directivos no se preocupan de saber lo que hacen los investigadores sobre el terreno. O de acercarse a un colegio para conocer los casos de abuso. Una manera de evitar que los menores de 14 años utilicen las redes sería la exigencia por parte de estos gigantes informáticos de un DNI digital para poder registrarse, lo que "evitaría muchísimos delitos entre menores", concluye Arén. Pero no hay interés en ello.

Con el panóptico, una estructura ideada por el británico Jeremy Bentham, explicado en su obra a finales del siglo XVIII, comenzó la vigilancia clásica. Se trataba de una torre situada en el centro de un edificio circular con amplias ventanas hacia el círculo interior. El edificio externo estaba dividido a su vez en celdas con ventanas tanto al exterior como al interior. Desde la torre, una persona podía vigilar a cualquiera que estuviera encerrado en ellas, sea un preso, un enfermo mental o un estudiante. Al entrar la luz del exterior, las figuras resultantes del contraluz facilitaban esa vigilancia, que no tenía necesariamente que resultar opresora. El vigilante cuidaba así de los habitantes del edificio, de los pacientes de un hospital o presos.

Si caminamos por algunas calles céntricas en Madrid, como Montera, Ballesta, Lavapiés, Azca o la Plaza Mayor, observaremos los tentáculos del panóptico actual, las cámaras blancas: algunas en forma de campana o tubo, suspendidas de un saliente atornillado a las paredes en las esquinas. La Policía Municipal gestiona 219 cámaras que enfocan las calles desde el Centro Integrado de Señales de Vídeo (CISEVI). El panóptico digital del siglo XXI es una sala repleta de pantallas encendidas las 24 horas. Fuentes de la policía aseguran que las imagenes se guardan durante una semana y luego se borran, aunque las grabaciones de las cámaras situadas en Azca se almacenan durante un mes. En España, la ley reconoce que cualquier ciudadano puede ejercer los derechos de acceso y cancelación de esas imagenes si ha sido grabado en la calle. Desde la policía se asegura que tendrá que llevar consigo una orden judicial.

En Reino Unido, de acuerdo con la Asociación Británica Industrial para la Seguridad, podrían operar un total de 5,9 millones de cámaras públicas y privadas. El número exacto se desconoce. Eso significaría una cámara por cada 11 británicos. Londres es la ciudad más vigilada de Occidente. La consultora global IHS estima que en el mundo hay unas 245 millones de cámaras de vigilancia. Asia contabiliza el 65% de las instaladas que funcionan actualmente.

Pero en este mundo dominado por el panóptico digital nos hemos convertido también en los que vigilan, en los observadores, señala Jorge Lozano, semiólogo y catedrático de Teoría de la Información de la Facultad de Periodismo de la Universidad Complutense de Madrid y autor del libro *El discurso histórico* (Sequitur, 2015). Habla de "prosumidor", una mezcla entre consumidor y productor, aludiendo a Marshall McLuhan.

Sigue.../...

El Gran Hermano de Orwell al que tenían acceso unos pocos para observar a muchos se ha democratizado. "Ahora es el nombre de un programa en el que todos, una audiencia de millones de telespectadores, observan a cuatro personas debajo de un edredón".

Un DNI digital para registrarse en redes sociales evitaría muchos delitos entre menores"

Nos vigilan, pero también vigilamos. En tiempos en los que los políticos blanden la transparencia como remedio a todos los males. Y como consecuencia de ese anhelo de transparencia, sentimos asfixia ante la invasión de nuestra privacidad. ¿Se ha destruido sin remedio? Para Bruce Schneier, "la gente no lo cree así. De lo contrario, dejarían de blindar su desnudez".

El Centro Pew de Investigación elaboró recientemente un informe y consultó a decenas de expertos. Surgieron dos grupos de opinión, los pesimistas y los medianamente optimistas. Entre los primeros, la sensación es que las montañas de metadatos cibernéticos han sepultado nuestra privacidad. "El Gobierno y la industria se han aliado para eliminar casi en su totalidad la privacidad de los consumidores y los ciudadanos", comentó Clifford Lynch, presidente de la Coalición Networked Information y profesor adjunto de la Escuela de Información de la Universidad de California en Berkeley. En el otro lado está Jim Hendler, uno de los arquitectos de Internet y profesor de Ciencias de la Computación del Instituto Politécnico Rensselaer, en Nueva York.

"Habrá un progreso significativo en este área y muchos asuntos concernientes a lo privado que van a evolucionar. La gente será cada vez más consciente de cómo se va a usar su información, a quién se le permite recolectarla y qué derechos podrán ejercer en el caso de que se produzcan violaciones; sin embargo, y dada la cantidad de información personal que estará disponible, también crecerá el potencial para cometer abusos". Kate Crawford, investigadora del Centro Microsoft de Nueva York, manifestó que "en los próximos 10 años se desarrollarán más tecnologías de la encriptación y servicios de *boutique* para aquellos que estén dispuestos a pagar para un mejor control de sus datos". Habrá una privacidad para ricos y otra para pobres. La privacidad se convertirá en un artículo de lujo.

Jorge Lozano, semiólogo, argumenta que la frontera entre lo público y lo privado ya empezó a difuminarse con la aparición de los medios de comunicación. "Nos queda nuestra esfera íntima". Y señala la obsesión actual por la cantidad de datos y metadatos. Ahora es posible grabarlo todo. Un exabyte equivale a 500.000 millones de páginas de texto. Toda la información que circula en Internet en este 2015 podría ser de unos 76 exabytes. "Google dispone de servidores suficientes para almacenar 15 exabytes en todo el mundo", según Schneier. Pero ¿qué se debe conservar? ¿Todo? ¿Y qué se debe descubrir o revelar? Lozano cita el caso de Wikileaks y los 250.000 documentos hechos públicos por las filtraciones de Julian Assange. "Se dijo en su momento que eran un paraíso para el historiador. Pero esto es falso. Ningún historiador trabaja con tanta cantidad de datos. Esos documentos privadísimos escondidos en las embajadas, los mismos documentos que Hillary Clinton hizo que considerara a Assange como un terrorista, no han descubierto ningún secreto. Decían lo que ya se sabía, como lo ha demostrado Umberto Eco".

Este semiólogo español encabeza un grupo de investigación cuya conclusión sorprende: a más transparencia, más opacidad. "Estamos exagerando el valor de la transparencia como si fuera un valor utópico". Por ello defiende el valor de la pertinencia, lo que debe descubrirse. Y no duda en afirmar, en estos tiempos en los que se clama por más transparencia, que "el secreto es la mayor conquista de la humanidad", citando al filósofo Georg Simmel. La privacidad nunca volverá. Si hoy día proclamamos que somos partidarios del secreto, quizá se nos tilde de políticamente incorrectos. Lo cierto es que todas las sociedades han abrazado al secreto para funcionar. Lozano nos recuerda finalmente lo que ya dijo Agustín de Hipona, el gran pensador del cristianismo y uno de los padres de la Iglesia, en su obra sobre la mentira *De Mendacio*. "Está prohibido mentir porque es un pecado contra Dios, pero no está dicho que estemos obligados a decir la verdad. De ahí la importancia del secreto".

elpaissemanal@elpais.es