Lo sabe
sobre u

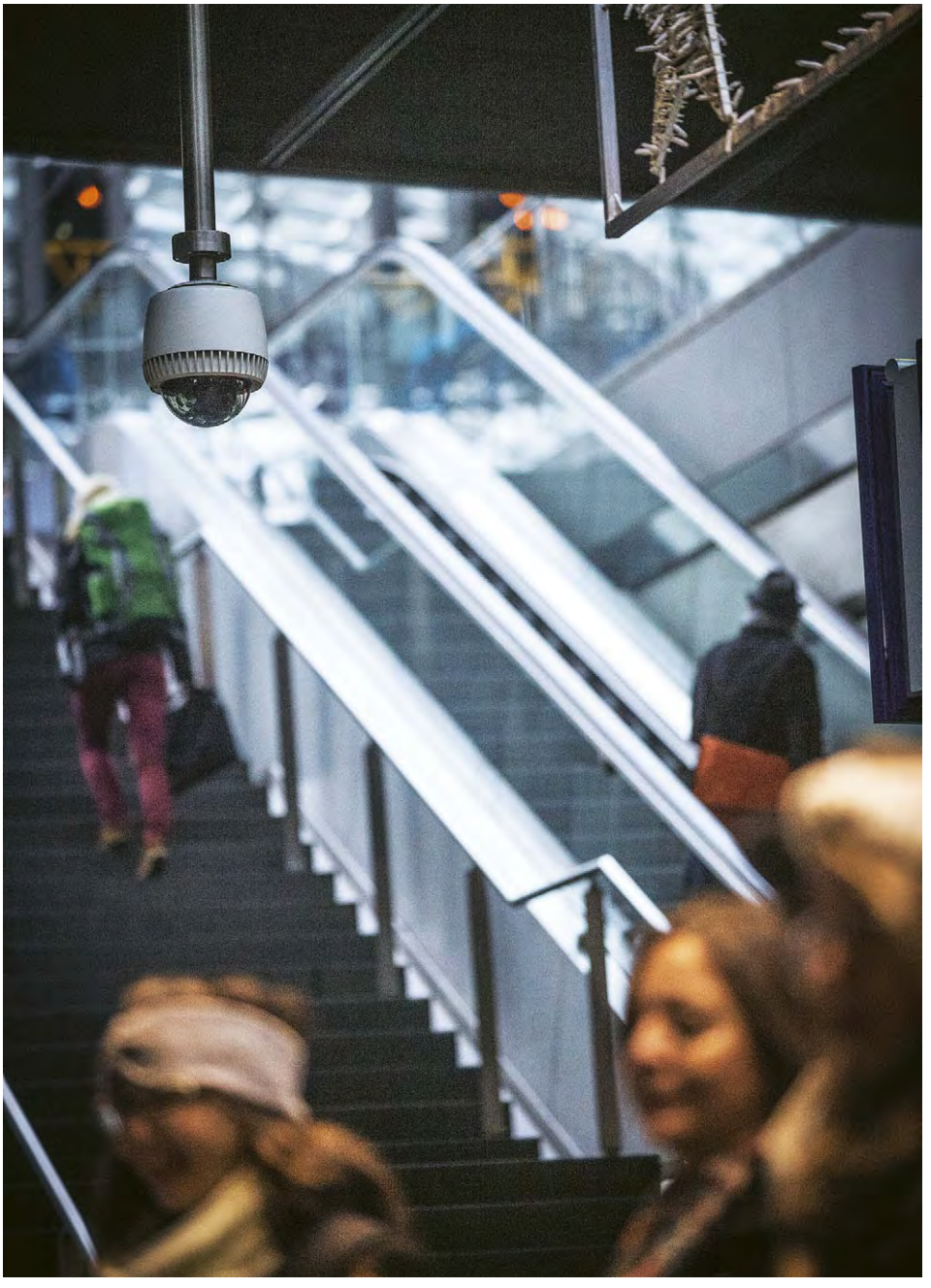
en todo usted

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. Un paso más hacia el cumplimiento de la profecía orwelliana.

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.

El salto hasta 2015 desde la distopía de la sociedad de *1984,* de George Orwell, repleta de recursos increíbles para la vigilancia, nos

FOTOGRAFÍA DE LA DOBLE PÁGINA ANTERIOR DE **JOHANNES ARIT (LAIF).** ESTA PÁGINA: **DOMINIK BUTZMANN (LAIF)**

“LOS SERVIDORES CONOCEN HASTA A LA PERSONA CON LA QUE DUERMES”

PÁGINA ANTERIOR
Vigilados. Cámaras controladas por la policía en Alemania.

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. 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 Applied,* 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”.

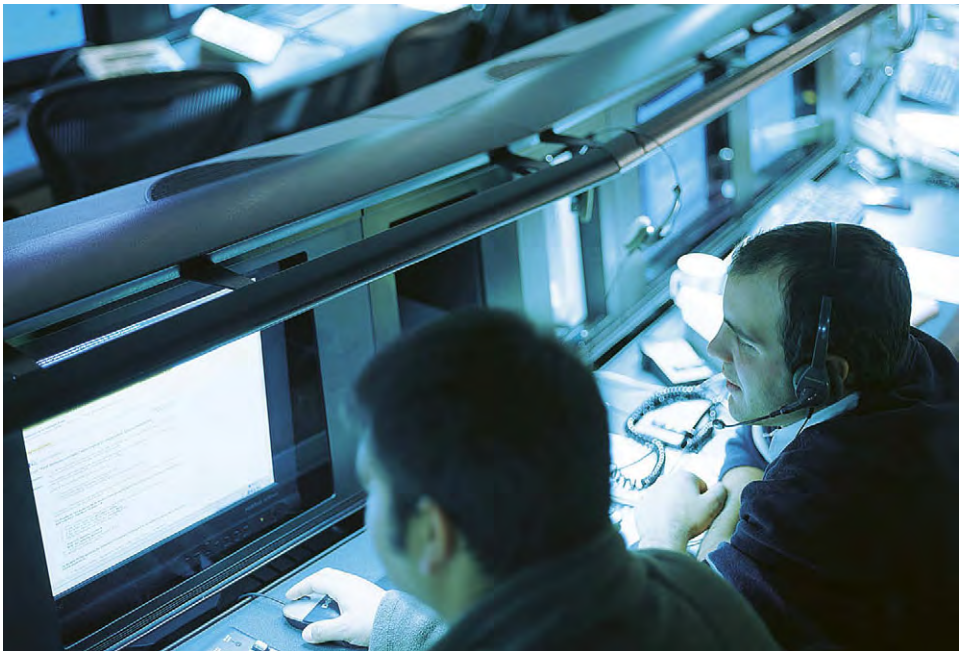
Los consumidores ordinarios hemos dejado de ser clientes para convertirnos en productos por la información que generamos. Cuanto más sepan de nosotros, más jugosos serán los beneficios en el mercado digital. ¿Quiénes se benefician y qué datos manejan exactamente?

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. 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...

HAY COMPAÑÍAS QUE OFRECEN A OTRAS EMPRESAS LA BÚSQUEDA DE PERSONAS A PARTIR DE METADATOS



Seguridad. Empleados de la corporación Symantec analizan datos para la protección de clientes ante ataques de piratas informáticos.

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 múl- →

FOTOGRAFÍA DE **SYMANTEC ('THE NEW YORK TIMES')**

tiple; 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. 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.

"LAS GRANDES CORPORACIONES TOMAN DECISIONES POR NOSOTROS SIN CONTAR CON NOSOTROS"

Circuito cerrado. Escena en el distrito financiero de La Defense, en París.

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 la 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.

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.

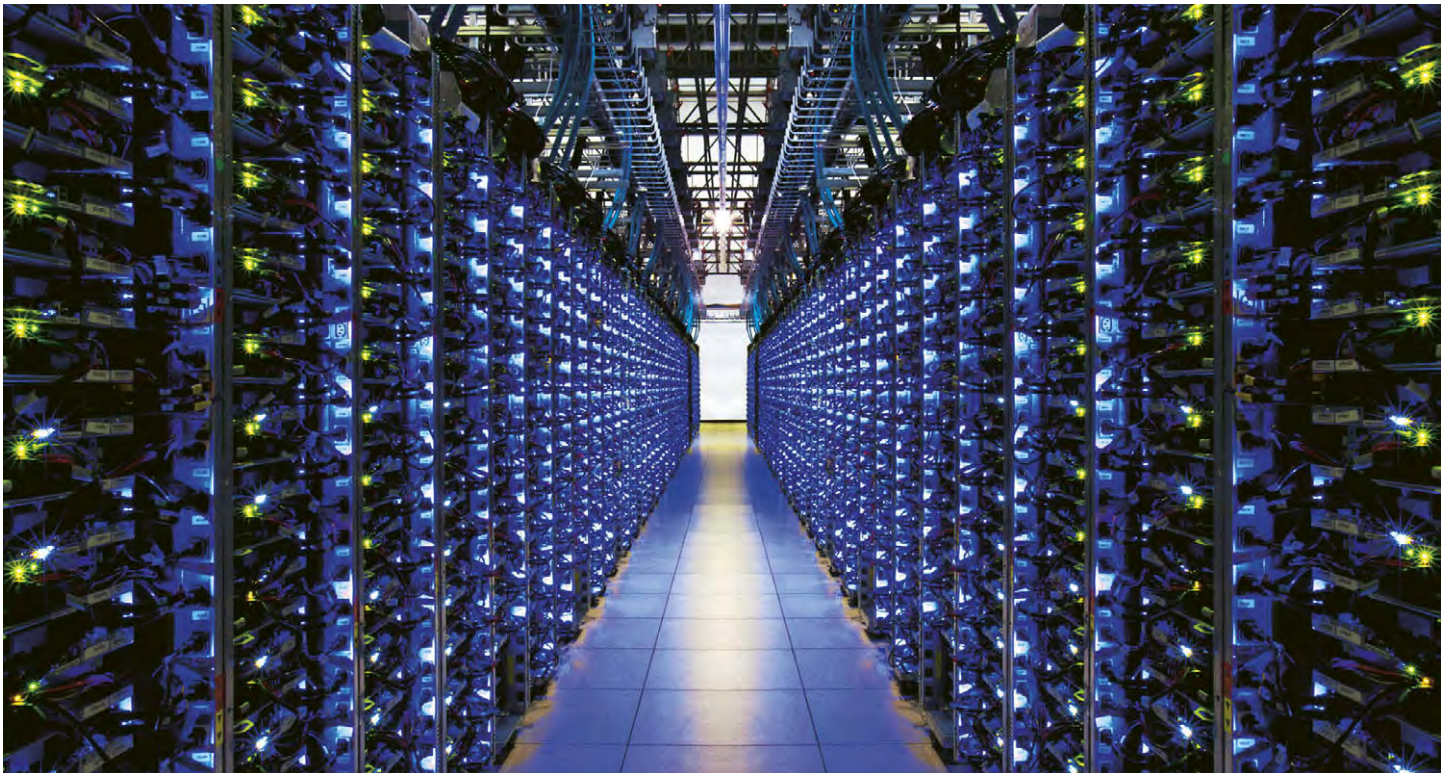
Esta responsable policial imparte charlas en los colegios para paliar el desinterés de las compañías de las redes sociales en explicar los peligros a los menores. Y narra situaciones antes inimaginables. Padres cuyos hijos recibían quimioterapia que contaban en sus mensajes de WhatsApp el nivel de los 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.

"UN DNI DIGITAL PARA REGISTRARSE EN REDES SOCIALES EVITARÍA MUCHOS DELITOS ENTRE MENORES"

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



Servidores. Centros de datos de la compañía tecnológica Google situados cerca de Atlanta (EE UU).

FOTOGRAFÍA DE **CONNIE ZHOU ('THE NEW YORK TIMES' / CONTACTO)**

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. 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".

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.

HAY 245 MILLONES DE CÁMARAS DE VIGILANCIA REPARTIDAS POR EL MUNDO. EL 65% DE ELLAS EN ASIA

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" ●