VIGILANCIA MASIVA

Con la excusa de la seguridad pública y la lucha antiterrorista, cada vez son más sofisticadas y poderosas las tecnologías de control y espionaje que gobiernos de todo el mundo emplean con los ciudadanos. Apenas podemos mover un dedo sin que quede constancia de ello, sobre todo, en el mundo digital. ¿Deberíamos resignarnos a renunciar a nuestro derecho a la privacidad?

Texto de
LAURA G. DE RIVERA

REC

Hoy, casi resultan obsoletos los métodos de Echelon, la gigantesca red de espionaje, análisis e interceptación de señales electrónicas que, desde la guerra fría, EE. UU. tiene a medias con Canadá, Reino Unidos, Nueva Zelanda y Australia.

SHUTTERSTOCK

Latifa deja su smartphone en el hotel. Sabe que existen sistemas, como StingRay, capaces de interceptar las comunicaciones móviles y, cómo no, localizar su posición, incluso, si lleva el dispositivo apagado. También, sabe que los servicios de inteligencia estadounidenses y británicos, entre otros, tienen métodos para activar a distancia el micrófono del teléfono y, así, grabar conversaciones. O la cámara, por eso siempre la lleva tapada con una pegatina opaca. Tiene una reunión importante, en la que decidirá con el resto de cabecillas del grupo activista al que pertenece qué acciones van a tomar en defensa de los derechos civiles, en el próximo congreso de la Organización Mundial del Comercio. Debe ser cuidadosa, si no quiere que sus planes sean anticipados por el férreo equipo de seguridad.

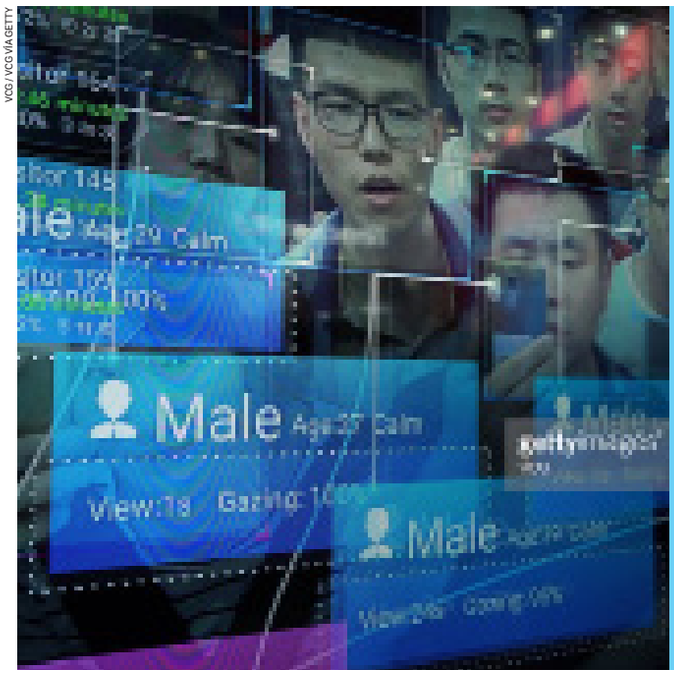
Usa internet solo a través de la red anónima Tor, para que nadie pueda rastrear su IP. Tampoco emplea correos gratuitos como Gmail, pues entre las condiciones de servicio de Google está su acceso al contenido de los mensajes privados y la entrega al gobierno estadounidense esta información personal de sus usuarios, sin previo aviso. Desde hace mucho, solo se comunica con un sistema de correo cliente y encripta todos mensajes con el códido abierto PGP. Además, cuando tomó el avión para llegar hasta la ciudad donde se celebra la cumbre, Latifa llevaba un móvil y un portátil nuevos sin ninguna app que pudiera comprometer datos sensibles, porque sabe que los agentes de aduanas y fronteras de muchos aeropuertos obligan a los sospechosos –de terrorismo, disidencia, inmigración ilegal...– a entregar sus dispositivos móviles y dar las contraseñas, sin necesidad de una orden judicial. "Queremos tener acceso a sus redes sociales, contraseñas. ¿Qué hacen en ellas, qué dicen? Mantener a los estadounidenses seguros y hacer cumplir las leyes del país en un mundo cada vez más digital depende de nuestra capacidad de examinar todos los materiales", señalaba en una entrevista para la *BBC* el director del departamento de Seguridad Interior, John Kelly, hablando de la práctica de revisar portátiles y móviles en la aduana de los aeropuertos de EE. UU. "Si no quieren cooperar, entonces, no entran", advierte.

PERO LOS PLANES DE LATIFA dan al traste cuando es detectada por las cámaras instaladas en puntos estratégicos de la ciudad, con un sistema de inteligencia artificial capaz de reconocer rostros. ¿Suena a película? Latifa es el único personaje ficticio del relato. El resto, toda la tecnología de vigilancia de la que hablamos, es real. Existe y se usa activamente en medio mundo.

China se lleva la palma, con el sistema de videovigilancia más sofisticado del planeta: 170 millones de cámaras CCTV –circuito cerrado de televisión– y una previsión de 400 millones más en los próximos tres años. En la ciudad

THOMAS TRUTSCHEL / PHOTOTHEK VÍA GETTY

Edward Snowden tuvo que huir de EE. UU. para no ser juzgado por un tribunal militar por haber sacado a la luz el espionaje de la NSA a los ciudadanos.



VCG / VCG VIA GETTY

Fichados

China ha empezado a expedir carnets de "crédito social" con puntos a cada ciudadano en función de sus estudios, sus deudas, locales que frecuenta, webs que visita, métodos de control de natalidad que usa, creencias religiosas, problemas de salud, salario que cobra, comentarios en las redes...

Y es que cada vez hay más datos sobre ti que sirven para identificarte y tenerte fichado. Incluso, investigadores de la Universidad de Standford diseñaron, a finales de 2017, un programa para distinguir si una persona es hetero u homosexual solo a partir de una foto de su cara, con un 81% de aciertos para los hombres y un 74% para las mujeres. "Esta tecnología no solo puede alentar la discriminación, también puede poner el peligro la vida de personas que viven en regímenes brutales donde la homosexualidad se considera un delito", denuncia el grupo en defensa de los derechos civiles The Human Rights Campaing.

Mientras, cada vez más dispositivos registran nuestros datos biométricos, como el iris o la huella digital. "Son unos datos muy personales y los cedemos inconscientemente a cambio de confort", nos advierte la experta en seguridad Paula de la Hoz.

de Guiyang, la policía guarda un catálogo digital de todos y cada uno de los ciudadanos: cada cara está vinculada a su número de identidad... y todos sus movimientos.

El periodista de la *BBC* John Sudworth lo probó en sus propias carnes cuando, después de dejar que la policía le tomara una foto, se sumergió en la marea humana del centro de la ciudad, para comprobar si de veras tan fácil era localizarlo. Siete minutos fue lo que el programa de IA de videovigilancia china tardó en identificar su rostro, determinar su localización entre el gentío de una estación de autobuses, avisar a la central y rodearlo con un grupo de agentes.

EL OBJETIVO DE ESTA RED DE CCTV de inteligencia digital, según declaraciones de Meng Jiazhu, secretario del Comité Legal y Político del partido Comunista, es proteger la "estabilidad social" y "poner orden... en la información fragmentada para delimitar la identidad de una persona". La idea, monitorizar y predecir las actividades de activistas y personas con ideas "extremistas". Para ello, "analizamos a los perfiles sospechosos, los observamos y advertimos a la policía de su presencia, teniendo en cuenta características que incluyen etnia o historial delictivo o cualquier cosa que resulte anormal". A Sophie Richardson, directora en China de Human Rights Watch, no le parece un buen plan: "Da miedo que las autoridades chinas estén recogiendo y centralizando todavía más información sobre cientos de millones de ciudadanos, identificando a personas que se desvían de lo que ellos consideran pensamiento normal", denuncia. Como guinda, un comunicado de prensa oficial de la Ciudad de Xuzho reconocía sin sonrojo que, para saber más sobre lo que hacen sus ciudadanos, la policía compra información a terceros, que incluye "datos sobre la navegación en internet y registros de envíos y transacciones con las principales compañías de comercio electrónico". Pero, quizá, de lo que más se enorgullece el servicio de "Nube Policial" chino es de su capacidad para trazar mapas de relaciones, es decir, el entramado de personas con las que alguien habla o se reúne. Uniendo todas las piezas de vínculos sociales, así, es posible detectar quiénes serían los líderes de un grupo disidente, por ejemplo. Un arma de valor incalculable para descabezar células terroristas... o grupos pacifistas en defensa del Tíbet libre o de la libertad de expresión.

La idea les encanta a todos los países totalitarios, por supuesto. Arabia Saudí e Irán han invertido millones de dólares en sistemas de videovigilancia. Mientras, Corea del Norte, Eritrea, Turkmenistán, Siria, China, Vietnam y Sudán se llevan la palma en cuanto a censura on line y persecución de blogueros disidentes, según la lista de enemigos de internet de Reporteros Sin Fronteras. Por su parte, el gobierno ruso le ha puesto una multa de 11.500 euros al servicio de mensajería instantánea Telegram por negarse a darle las contraseña para desencriptar sus mensajes, y amenaza con echarlo de sus fronteras. Y, cómo no, el país de la Gran Muralla usa un cortafuegos gigante para filtrar todo el contenido que pasa por su territorio. Hasta tiene una brigada de 30.000 agentes especializada en perseguir a los que escriben algo que pueda considerarse reprimible. Por sus manos pasaría el bloguero Yang Tongyan, que el año pasado murió en la cárcel. En Arabia Saudí, tampoco se andan con chiquitas: Raif Badawi, fue sentenciado en 2015 a 1.000 latigazos y 10 años de prisión por los comentarios políticos que hizo en su blog.

Espeluznante, ¿verdad? Menos mal que nosotros vivimos en países libres y democráticos, donde los gobiernos protegen el derecho a la intimidad, a la libertad de expresión, el tráfico de datos personales... ¿Seguro? Pues no. Los países occidentales son expertos desde hace décadas en el control de todas las comunicaciones digitales, con una tecnología que dejaría boquiabierto al propio James Bond. En cabeza, el Pentágono estadounidense, después del 11 de septiembre de 2001, decidió que

Las calles de la ciudad china de Guiyang están sembradas de cámaras con un sistema de reconocimiento facial inteligente

»

Desde el aire

¿Qué puede hacer un robot volador del tamaño de una libélula con una cámara con zoom milimétrico y de visión nocturna? Para empezar, verlo y grabarlo casi todo. El MQ-9 Reaper de la NSA estadounidense puede identificar un objeto del tamaño de un libro desde una altitud de 60.000 pies y percibir el calor de un cuerpo humano desde una distancia de 60 kilómetros. Una idea muy práctica para fines militares y de espionaje en zonas de conflicto bélico. De hecho, fue empleada por el ejército español en Afganistán para prevenir emboscadas. Chinos, iraníes, israelitas y estadounidenses se llevan la palma en drones armados, para realizar bombardeos selectivos. También, son perfectos para controlar la inmigración ilegal, para buscar terroristas por el desierto... o para espiar lo que hace el vecino. Como el Black Hornet –en la imagen– un coqueto mini helicóptero que el ejército británico utiliza para ver qué pasa por encima de los muros de propiedades privadas, siempre con la excusa de la seguridad nacional. ¿Pero qué pasa con la privacidad? ¿Y si, en vez de un yihadista haciendo bombas, al otro lado de la valla solo está tu abuela haciendo *topless*?

BEN BIRCHALL / PA IMAGES VÍA GETTY

SPENCER WHALEN / EYEEM / GETTY

Existen programas capaces de hackear y activar a distancia la cámara del móvil. Unidos al reconocimiento facial, se pueden usar para identificar a todas las personas que te rodean.

la única forma de prevenir futuros ataques terroristas era extremar la vigilancia.

Si no, se que lo digan a Edward Snowden, informático y ex agente de inteligencia, que tuvo que escapar de su país para no acabar encarcelado como su colega Chelsea Manning. Su pecado fue sacar a la luz los métodos de vigilancia global del programa PRISM, que le da acceso directo a la NSA –Agencia de Seguridad Nacional– a toda la información –datos personales, contenido de los mensajes, actividades on line, conversaciones telefónicas, registros... todo– que guardan sobre sus usuarios compañías tecnológicas como Yahoo, AT&T, Microsoft, Google, Facebook y Apple. Lo hacen a través de las Cartas de Seguridad Nacional –National Security Letters–, órdenes de registro que no precisan autorización judicial. Además, la proveedora de servicios tiene prohibido advertir al usuario en cuestión de que ha cedido sus datos al gobierno.

"CRECÍ CON EL ENTENDIMIENTO DE QUE VIVÍA en un mundo donde la gente tenía libertad para comunicarse con otros con privacidad, sin ser vigilados o juzgados por estos sistemas sombríos cada vez que mencionamos algo que viaja por las redes de comunicación públicas", explicaba el joven informático en una entrevista con Glenn Greenwald para *The Guardian*. "A partir de ahora, cada frontera que cruces, cada compra que hagas, cada llamada que realices, cada toma de telecomunicaciones por la que pases, cada web que visites y cada correo que escribas estará en manos de un sistema cuyo alcance es ilimitado", advirtió Snowden a la documentalista Laura Poitrás, cuando la eligió como intermediaria para a dar a conocer los secretos de la NSA. De hecho, Poitras, que ganó un Oscar por su trabajo, se pasó 6 años en la lista negra de enemigos de la seguridad pública, en EE. UU. No podía pasar por un aeropuerto sin que registraran su equipaje y le confiscaran durante horas, o días, cámaras, ordenador, teléfono... para revisar su contenido y ver si atentaba contra la seguridad nacional.

PARA ESO, EXISTEN PROGRAMAS DE SOFTWARE FORENSE, capaces de recolectar todas las fotos, contactos, incluso contraseñas de correo electrónico y redes sociales, en cuestión de minutos. "El kit completo permite a sus clientes corporativos, de la policía o del gobierno acceder a smartphones y tabletas, hacerse con contraseñas de *backups* y descodificar *backups* encriptados, ver y analizar información almacenada", anuncia el fabricante Elcomsoft en su web.

Otro jugoso objeto de vigilancia para las agencias de inteligencia occidentales son los metadatos. Se trata de establecer comunidades de intereses, gente que se llama con regularidad o que participa en los mismo foros... Así, la herramienta llamada Co-traveler de la NSA es capaz de trazar mapas de las relaciones entre individuos con la excusa de que encontrar nodos en las redes digitales, siguiendo el entramado de comunicaciones de un sospechoso, puede ayudar a localizar grupos terroristas o disidentes. La pregunta es ¿sospechoso de qué? ¿De poner bombas... o de ser activista de Greenpeace, anti-Trump, homosexual, o mujer liberada en un país islámico?

Las proveedoras de servicios de internet pueden ceder nuestros mensajes privados al gobierno de EE. UU. sin avisarnos

Por ejemplo, la base de datos Talon, autorizada por el ministerio de Defensa de EE. UU. después del 11 de septiembre de 2001, con la misión de reconocer y evaluar información sobre posibles amenazas, incluía en su lista de sospechosos a personas que habían asistido a manifestaciones pacifistas, catalogados como no afines al sistema. La opinión pública obligó a cerrar Talon, que ahora ha sido sustituida por el sistema Guardian del FBI.

Y ES QUE EL FBI Y LA NSA gastan miles de millones de dólares en revisar y analizar de forma automática la ingente cantidad datos y metadatos en internet, a través de programas como Carnivore, NarusInsight o Echelon. En la misma línea, poseen una enorme base de datos de ciudadanos dentro del programa Infragard, que ha firmado acuerdos con unas 34.000 empresas privadas para "compartir información" sobre sus clientes: hábitos de compra, transacciones....

Por si fuera poco, las dos principales empresas de telecomunicaciones de EE. UU., AT&T y Verizon, tienen contratos con el Centro de Recogida de Datos de Telecomunicaciones del FBI para registrar y ceder el contenido de las llamadas de sus usuarios, a cambio de 1,8 millones de dólares al año cada una, según datos publicados en *Wired* por Ryan Signel.

"Nunca digas nada en un mensaje electrónico que no te gustaría ver publicado con tu nombre en la primera página de la edición de mañana del *New York Times*", advierte el coronel David Russel, ex director del departamento de proceso de información de DARPA, la agencia de I+D para uso militar gringa. Y es que, entre otras consecuencias peligrosas para las libertades personales y políticas, los sistemas de vigilancia digital crean una sensación general de estar siendo observados. Esto hace que la gente de a pie se autocensure.

Un estudio de Jonathon Penney, publicado en *Berkeley Technology Law Journal*, en 2016, comprobó que el tráfico a Wikipedia se redujo un 20 % después de las revelaciones de Snowden, en lo relativo a consultas acerca de terrorismo, incluidas las que hacían alguna referencia a "al Qaeda", "coche bomba" o "talibán". Además, en una encuesta de 2015, Penney sacó a la luz que el 13 % de los estadounidenses reconocía haber empezado a "evitar usar ciertos términos on line". "Si, por miedo a ser vigiladas, juzgadas o etiquetadas, las personas dejan de buscar información sobre cuestiones políticas importantes como terrorismo y seguridad nacional, ello supone una amenaza real al debate democrático sano", denunciaba el investigador. En la misma línea, un estudio de Catherine Tucker, profesora de Derecho en el Massachussetts Institute of Technology, concluyó que los informes de Snowden sobre la intromisión del gobierno en la privacidad habían disminuido significativamente las búsquedas en Google sobre temas políticamente sensibles –un 5 %–, pero también sobre cuestiones "íntimas", que pudieran dar pistas sobre datos personales o de salud del usuario –por ejemplo, el término "anorexia"–.

EN 1996, UN INGENUO LIBERTARIO, John Perry Barlow, uno de los fundadores de Electronic Frontier Foundation, publicó la *Declaración de Independencia del Ciberespacio*, donde afirmaba que internet es "un espacio social global contruido por todos [...] por naturaleza, independiente de las tiranías". Sin embargo, no hemos elegido a los gigantes tecnológicos ni a los dictadores que nos imponen sus normas, sin respeto por el derecho a la intimidad o la libertad de expresión.

"La tecnología no es neutral. Tiene la ideología de los que la crean", apunta a *Muy Interesante* Meskio Sattler, programador de la plataforma de privacidad digital Leap.se. Y la fiebre por el control digital no sale solo de los gobiernos, también ha infectado a las empresas, y hacia sus propios empleados. Según Sattler, algunos trabajadores de Amazon, por ejemplo, llevan un dispositivo que va marcando sus pasos por las oficinas. "Así el jefe puede ver y evaluar las cosas que has hecho y reprenderte si resulta que te has parado demasiado tiempo charlando en el pasillo", explica. Los mensajeros de Deliveroo, por su parte, "van a cuestas con una aplicación en el móvil para cronometrar todos sus tiempos, en la que deben ir marcando cuándo llegan al portal, cuándo les responden a telefonillo...", añade. Asimismo, según un informe de la American Management Association, en EE. UU., el 40 % de las compañías monitorizan el tráfico de emails de sus trabajadores y el 66 %, sus conexiones a internet.

Pero estemos tranquilos. Nosotros, la gente normal, los que no somos ex informáticos de la CIA, ni empleados de Amazon, ni construimos bombas... no tenemos nada que temer. ¿Seguro? Como remarcaba Snowden, "no preocuparse de la privacidad porque no tienes nada que esconder es como no defender la libertad de expresión porque no tienes nada que decir".