Economist Intelligence Unit

TECNOLOGÍA Y ESPIONAJE

Aumenta la posibilidad de abusos con las nuevas tecnologías para recabar información personal

Visitantes examinan un UAV (vehículo aéreo no tripulado, por sus siglas en inglés) elaborado por EADS, empresa líder de la industria aeroespacial, durante una exhibición reciente en París ■ **Foto Reuters**

Vivir con el Hermano Mayor

Antes era fácil saber si estaba uno en un país libre o en una dictadura. En un Estado policiaco al viejo estilo, los soplones están por todas partes, ya sea en persona o en una red de informantes que penetra oficinas, comunidades y familias. Señalan lo que pueden sobre nuestras opiniones políticas y debilidades personales, si tenemos el poco cuidado de expresarlas en público. Lo que no oyen en el café o la cantina lo conocen leyendo nuestras cartas o interviniendo nuestro teléfono. Luego, la información recabada se almacena en millones de papelitos amarillos, escritos a máquina o a mano; desde el punto de vista de un dictador al viejo estilo, el acceso exclusivo a estos archivos es un instrumento tan poderoso como cualquier cámara de tortura. Sólo cuando el régimen cae, los archivos se destruyen o se abren, y entonces las personas pueden ver quién de sus amigos era informante.

En la actualidad, la información sobre ubicación, compras, comportamiento y vida privada de las personas se recopila, almacena y comparte en una magnitud que ningún dictador de la vieja escuela pensó posible alguna vez. Los gobiernos sostienen que tienen que recabar esta información para luchar contra el terrorismo o proteger la salud pública; las corporaciones dicen que lo hacen para proporcionar mercancías y servicios de manera más eficiente. Pero la facilidad para obtener esta clase de información y procesarla –y sobre todo, su aceptación por el público– es algo asombroso si se compara con hace una década. Y tampoco se limita a una región o a un sistema político.

En China, millones de ciudadanos están siendo obligados a obtener tarjetas "de residencia" de alta tecnología. Estas tarjetas contienen datos de identidad étnica, religión, estudios realizados, antecedentes penales e, incluso, historia reproductiva; refinamiento propio de los documentos de identidad de los regímenes comunistas.

Gran Bretaña solía estar orgullosa de respetar más la privacidad que otras democracias. Pero en cuanto a las cámaras de vigilancia se refiere, los británicos no objetan demasiado. Estas cámaras de vigilancia "parlantes", equipadas con altavoces, permiten a sus operadores humanos dar una reprimenda a quienes son sorprendidos tirando basura, orinando contra una pared o en otro comportamiento "antisocial".

Una tecnología aún más inteligente –diseñada para enfrentar las guerras del siglo XXI– se usa ya en la lucha contra delitos tanto graves como menores. En Gran Bretaña, Italia y Estados Unidos, la policía experimenta con aviones abejorros en miniatura a control remoto, equipados con cámaras de video y visión infrarroja nocturna, para detectar comportamientos "sospechosos" en muchedumbres. De menor peso que una bolsa de azúcar y tan silencioso que no puede ser oído cuando está a 50 metros del suelo, el UAV (vehículo aéreo no tripulado, por sus siglas en inglés) puede volar incluso sin que se vea, en virtud de las imágenes que envía a un operador de campo equipado con lentes especiales. MW Power, la empresa que distribuye la tecnología en Gran Bretaña, tiene planes para añadir un aerosol de "agua inteligente" que se lanzaría a chorro sobre los sospechosos, impregnado su piel y ropa con marcas genéticas, lo que permitiría a la policía identificarlos más tarde.

Casi siempre, los beneficios de la tecnología electrónica y la evidente necesidad de combatir a los delincuentes parecen pesar más que cualquier preocupación sobre su uso. Ésta es una situación reciente. A finales de los años 90 era común escuchar que la derecha religiosa estadunidense lanzaba advertencias oscuras sobre la utilización de códigos de barras electrónicos en el comercio: ¿acaso no evocaban la "marca de la bestia", sin la cual "ningún hombre podría comprar o vender", profetizada en el Apocalipsis? Pero los tecnófobos de hoy, religiosos o no, se han acostumbrado a dispositivos aún más atemorizantes.

Por ejemplo, los microchips de identificación de radiofrecuencia (RFID, por sus siglas en inglés) que se han usado tanto tiempo para rastrear mercancías e identificar animales domésticos, se implantan cada vez más en seres humanos. Se utilizan para que los trabajadores sociales estadunidenses sigan la pista de ancianos; para que los empleados tengan acceso a áreas de alta seguridad (en México y Ohio), e incluso para proporcionar a los dueños de clubes nocturnos la posibilidad de evitar colas a la entrada y prescindir de efectivo en la barra (en España y los Países Bajos). Algunas personas desean que a todos se les implante un RFID, en respuesta al robo de identidad.

Como nunca, en el mundo rico y no tan rico se utilizan dispositivos electrónicos para vigilar a ciudadanos ordinarios. Cámaras de circuito cerrado de televisión (Cctv) con visión infrarroja nocturna, observan detenidamente a los ciudadanos desde las esquinas de calles, bancos, aeropuertos y centros comerciales. Cada vez que alguien teclea una página *web*, hace una llamada telefónica, usa una tarjeta de crédito o marca su entrada al trabajo con una tarjeta de microchip, deja un rastro de información que puede seguirse más tarde. Todos los días, miles de millones de bits de información personal se almacenan, examinan, analizan y cruzan con otros datos y, en muchos casos, se usan para construir perfiles que predicen comportamientos. A veces esta información es acumulada por los gobiernos; la mayoría la recaban las empresas, aunque en muchos casos se les obliga a ponerla a disposición de las agencias policiacas y otros cuerpos estatales.

Siga la información

Entre más información se recabe y almacene, mayor es la probabilidad de "extracción de datos": la utilización de fórmulas matemáticas en el análisis de grandes conjuntos de datos para descubrir pautas y predecir comportamientos. Si el público de los países ricos tenía ciertas inquietudes sobre la legitimidad de este proceso, la mayor parte se evaporaron luego del 11 de septiembre de 2001, cuando muchos aceptaron que contra un enemigo mortal, integrado en una red mundial, toda estratagema era necesaria. Técnicas para procesar información personal que podrían haber provocado críticas antes de 2001 de repente parecieron indispensables.

Dos días después de los ataques a Nueva York y Washington, Frank Asher, ex narcotraficante que cambió al negocio de tecnología, decidió examinar la información recabada sobre 450 millones de personas por Seisint, su empresa privada de servicios de información, para ver si podía identificar a posibles terroristas. Después de asignar a cada persona puntos de riesgo con base en el nombre, religión, historial de viajes, preferencias de lectura, etcétera, obtuvo una lista de mil 200 "sospechosos", que entregó a la Oficina Federal de Investigación (FBI, por sus siglas en inglés). Sin que él lo supiera, cinco de los secuestradores terroristas estaban en su lista.

La FBI quedó impresionada. Renombrado Matrix (Multistate Antiterrorism Information Exchange, Intercambio de Información Antiterrorista entre Estados), el programa de Asher, ahora controlado por la FBI, pronto tendría acceso a 20 mil millones de bits de información, recabada, clasificada y analizada para predecir quién podría convertirse alguna vez en terrorista. Una nueva versión, denominada Sistema para Evaluar el Riesgo, o STAR por sus siglas en inglés, usa la información extraída de bases de datos privadas y públicas. Como la mayor parte de la información ya ha sido revelada a terceros –boletos de avión, expedientes laborales, alquiler de coches y similares– no está protegida por la Cuarta Enmienda de la Constitución estadunidense, así que no se requiere autorización judicial.

En una era en que los gobiernos están empeñados en frustrar posibles ataques, construir perfiles se ha convertido en un instrumento favorito. Pero aunque puede predecir el comportamiento de grandes grupos, esta técnica es "increíblemente inexacta" cuando se refiere a individuos, dice Simon Wessely, profesor de siquiatría en el King's College, de Londres. Bruce Schneier, gurú estadunidense de la seguridad, está de acuerdo. La extracción de enormes cantidades de datos para construir modelos de comportamiento bien establecidos, como el fraude con tarjeta de crédito, funciona muy bien, dice. Pero es "extraordinariamente incierto" cuando sondea conjuras terroristas, que son poco comunes y raras veces tienen un perfil definido.

Por ejemplo, Schneier señala el Sistema de Señalamiento Automatizado operado por los sistemas estadunidenses de aduanas y protección fronteriza, que asigna puntos de evaluación de riesgo terrorista a cualquiera que entre o salga de Estados Unidos (EU). En 2005 se procesó información de unos 431 millones de personas. Suponiendo, de manera poco realista, que un modelo preciso sea capaz de identificar terroristas (y personas inocentes) con una exactitud de 99.9%, esto se traduce en más o menos 431 mil falsas alarmas por año, las cuales, obviamente, requirieron investigación. Considerando la falta de credibilidad de la información sobre los pasajeros, el número real es, con toda probabilidad, mucho más alto.

A los individuos enlistados por los sistemas de perfiles terroristas no se les permite conocer sus puntos u objetar los datos, pese a que sus perfiles, que pueden compartirse con gobiernos federales, estatales y aun extranjeros, pueden dañar sus posibilidades de conseguir empleos en el gobierno, becas estudiantiles, contratos públicos o visas. Podrían incluso impedir que vuelen de nuevo. Esos errores son frecuentes, como el inconfundible senador Ted Kennedy lo descubrió por sí mismo. Durante 2004, en sólo un mes, cinco veces se le impidió tomar un vuelo porque el nombre "T Kennedy" había sido usado por alguien señalado como sospechoso de ser terrorista, en una lista secreta de "impedido para volar".

Vigilando a todo el mundo

Otra preocupación: antes, la información sobre personas solía recopilarse de manera selectiva (por ejemplo, seguir el coche de algún sujeto); ahora se reúne de forma indiscriminada. El mayor

▶

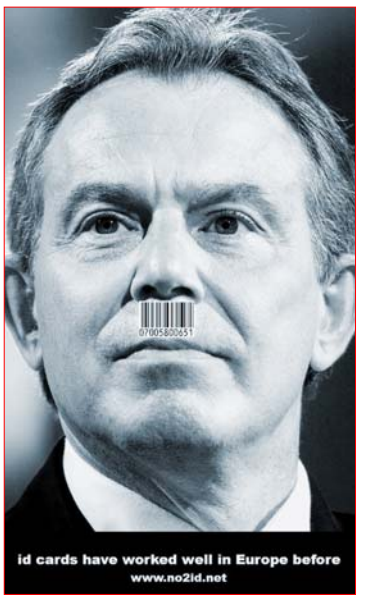
ejemplo de esa vigilancia universal es el extenso uso de cámaras de circuito cerrado. Con cerca de 5 millones de cámaras colocadas en lugares públicos, Inglaterra y Gales se encuentran entre los países más estrechamente vigilados del mundo, junto con Estados Unidos, país que cuenta con unos 30 millones de cámaras de vigilancia, una por cada 10 habitantes. Cada ciudadano inglés puede esperar aparecer ante una cámara un promedio de 300 veces al día. A pocos parece importarles esta situación, a pesar de que las investigaciones sugieren que las cámaras hacen muy poco para disminuir el total de delitos.

De cualquier forma, el movimiento británico "No a la Identificación" (NO2ID, por sus siglas en inglés), que pugna por detener los planes del gobierno de implantar el uso de tarjetas de identidad, afirma que las cámaras son un asunto de menor importancia frente a la creación de un "Estado apoyado por bases de datos", en el cual los archivos personales de cada ciudadano quedan en un registro y tienen un acceso demasiado fácil.

Junto con las huellas digitales, el ácido desoxirribonucleico (ADN) se ha convertido en una herramienta cada vez más popular para detectar la presencia terrorista y resolver delitos. En esto también Gran Bretaña es líder mundial, con una colección de muestras de ADN en su base de datos, creada en 1995, de 4.1 millones de individuos, es decir, 7% de la población. (La mayor parte de los otros países de Europa no tiene más de 100 mil perfiles de ADN en su base de datos). La británica incluye muestras de uno de cada tres hombres negros y cerca de 900 mil jóvenes entre 10 y 17 años de edad, todos marcados de por vida como delincuentes probables, debido a que la inclusión de sus datos indica que han tenido algún rozón con la ley. Esto se debe a que en Gran Bretaña se pide el ADN a cualquiera que sea arrestado por una falta "archivable", por lo general, alguna que conlleve una sentencia de reclusión, pero también incluye pecadillos como una borrachera y el escándalo en la vía pública. La muestra se guarda de por vida, aun si la persona nunca es consignada o es perdonada más adelante. Ninguna otra democracia hace esto.

En Estados Unidos, el banco de datos federal de ADN guarda 4.6 millones de perfiles, que representan 1.5% de la población. Pero casi todos son de delincuentes sentenciados. Desde enero de 2006, la FBI ha permitido que se tomen muestras de ADN a la hora del arresto, pero se pueden eliminar, a petición del inculpado, si no es consignado o se le absuelve. En Gran Bretaña, donde los ciudadanos no pueden pedir que se borren sus muestras de la base de datos, se ha propuesto que la mejor manera de evitar la discriminación es incluir a toda la población, así como el ADN de cuanta persona visite el país. Aunque dicha propuesta parece justa, resultaría demasiado costosa y se tornaría una pesadilla administrativa.

En la cultura popular, el uso del ADN se ha convertido en un asunto glamoroso. Los periódicos y la televisión cuentan cómo los policías usan el ADN para localizar secuestradores o exculpar a reos condenados a muerte. De acuerdo con una encuesta que la BBC realizó en su serie *Panorama*, dos de cada tres británicos apoyarían una nueva ley que exigiera a todo ciudadano dar una muestra de ADN para la base de



El ex premier Tony Blair en un fotomontaje publicado en 2006 a toda plana por el movimiento NO2ID, en protesta por la implantación de tarjetas de identidad en el Reino Unido ■ **Foto Biometrics.co.uk**

datos. Pero el ADN es menos confiable como herramienta de detección criminal de lo que la mayoría de la gente cree. Aunque casi nunca provee una lectura de un falso "negativo", puede producir, en cambio, falsos "positivos". El profesor Allan Jamieson, director del Instituto Forense de Glasgow, cree que se ha puesto demasiada fe en esta técnica. Jamieson afirma que una persona puede transferir su ADN a un lugar, o a una arma que él o ella nunca han visto o tocado.

El espionaje telefónico es fácil

Más perturbador resulta para la mayoría de estadunidenses los inmensos poderes que el gobierno se ha dado en los seis años pasados para espiar a los ciudadanos. Conforme a la Ley Patriótica, elaborada a la carrera tras los ataques de 2001, los servicios de inteligencia y la FBI pueden obligar ahora a terceras partes –proveedores de Internet, bibliotecas, compañías telefónicas y partidos políticos, entre otros–, a entregar información de cualquier persona sin orden judicial ni conocimiento del afectado, siempre y cuando las instituciones digan que la información se necesita para una "investigación autorizada" en conexión con el terrorismo internacional. (A principios de octubre, un tribunal federal de Nueva York consideró que esto es inconstitucional.)

De la misma manera, la casa o la oficina de una persona pueden ser registradas sin su conocimiento o sin orden previa. La ley también extendió la facultad del gobierno para interceptar correos electrónicos privados, así como llamadas telefónicas, aunque para esto último supuestamente todavía se requiere la orden de un juez. Pero so pretexto de su función de comandante en jefe en tiempos de guerra, George W. Bush decidió pasar por alto este requerimiento e implantó su propio programa de espionaje sin orden judicial.

El clamor que se dejó escuchar tras esta revelación fue ensordecedor, y el programa abortó. Pero en agosto, Bush aprobó una enmienda a la Ley de Vigilancia de la Inteligencia Extranjera, de 1978, la cual permitía interceptar sin orden judicial llamadas telefónicas y correos electrónicos si había una creencia "razonable" de que al menos alguna de las partes se hallaba fuera del país. Así que los estadunidenses comunes continuarán siendo espiados sin necesidad de órdenes, pero ya nadie protesta, porque ahora es legal.

¿Dónde está la orden?

De acuerdo con los defensores del espionaje sin permiso, expedir órdenes para toda la vigilancia que debe ejercer el gobierno limitaría de forma dramática el flujo disponible de datos de inteligencia. Argumentan que la privacidad no debe ser prioritaria. Pero, ¿en verdad se impediría la actuación de la ley si un juez emite una orden cada vez que se necesite? Abogados afirman que la tecnología ha convertido el espionaje en algo demasiado fácil, así que requerir las órdenes ayudaría a restablecer el equilibrio.

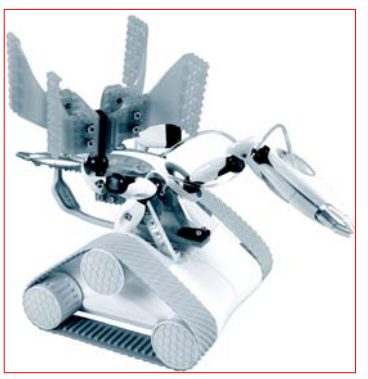
Gran Bretaña ha permitido por mucho tiempo el espionaje de sus ciudadanos sin orden judicial (sólo se requiere la autorización de la secretaria del despacho), y a pocas personas parece importarles. Lo que les preocupa es el volumen de información que se guarda de cada uno y el grado en que se ha vuelto accesible a un grupo todavía más grande de individuos y agencias. El gobierno desarrolla actualmente la primera base de datos del mundo que contendrá la información de cada menor de 18 años. La base de datos del Servicio de Salud Nacional, el mayor de su clase en Europa, contendrá los expedientes médicos de los 53 millones de personas que viven en Gran Bretaña y Gales.

Aún más discutible resulta el Registro Británico de Identidad Nacional, debido a que contiene hasta 49 diferentes asuntos de cada habitante del país. A partir de 2009, a todos se les dará una tarjeta de identidad biométrica "inteligente", vinculada con el registro nacional, la cual será necesaria para tener acceso a servicios públicos, como cirugías, oficinas de desempleo, bibliotecas y otros, de manera que dejen un rastro de datos electrónico nuevo y fácil de leer. Estados Unidos planea un sistema similar, con datos personales contenidos en una nueva licencia nacional de conductor que fungirá también como tarjeta de identidad.

Las compañías también juntan inmensas cantidades de datos. La mayoría de las personas ni siquiera se fijan en qué información entregan cuando usan su tarjeta de crédito, compran algo en línea o firman un préstamo. Tampoco tienen mucha idea del uso que dichos datos tendrán en lo sucesivo. No sólo las compañías "extraen" esos datos para dirigir de manera más efectiva su publicidad, sino también para dar a sus clientes más valiosos (por ejemplo, los que gastan más) un mejor servicio. También pueden "compartir" los datos con la policía sin permiso o conocimiento del dueño.

En la actualidad, los países más democráticos cuentan con leyes que garantizan la protección y/o la privacidad, ya que contienen reglas estrictas para la recolección, el almacenamiento y el uso de datos personales. También existe con frecuencia un comisionado nacional de información o privacidad que supervisa dicha protección (aunque no en EU). A las agencias de inteligencia, y con frecuencia a las autoridades judiciales, se les exime de respetar dichas leyes siempre que la seguridad nacional esté en juego. Pero por lo general se estipula que los datos deben usarse sólo para propósitos específicos, no deben conservarse más tiempo del necesario, y deben mantenerse precisos, actualizados y protegidos de espionaje no autorizado.

Todo eso suena muy bien.



Spykee, robot que cuenta con un sensor de movimiento, y ante determinadas circunstancias dispara una alarma y envía una fotografía a la dirección de correo electrónico que se le indique ■ **Foto Ap**

Pero una serie de filtraciones en los años pasados demuestra que ninguna información está nunca en verdad segura. Computadoras portátiles con información importante son robadas de autos, cintas de respaldo se pierden en el trayecto y los piratas cibernéticos pueden irrumpir en las bases de datos, aun en la del Pentágono. También están los "ataques desde el interior", en los cuales ciertas personas abusan del acceso que disfrutan gracias a su puesto. Hace poco se supo que trabajadores del Servicio de Salud de Gran Bretaña escudriñaron los detalles íntimos y médicos de una celebridad. Todo esto puede conducir a invasiones a la intimidad y al robo de identidades.

Ranas hervidas

Si el desgaste de la privacidad individual empezó mucho antes de 2001, se ha acelerado enormemente desde entonces. Y no siempre para mal: es posible que los atacantes suicidas, por su propia naturaleza, no sean detenidos por una cámara de circuito cerrado (aunque ésta hablara), pero defensores de la seguridad afirman que muchos planes terroristas han fracasado, y muchas vidas se han salvado, mediante el incremento del espionaje, la elaboración de perfiles y la búsqueda en asuntos privados. Pero, ¿cuál ha sido el costo para las libertades civiles?

La privacidad es un "derecho" moderno. Ni siquiera se menciona en la lista de demandas de los revolucionarios del siglo XVIII. De hecho, no se hizo explícito en las leyes y tratados hasta después de la Segunda Guerra Mundial. Pocas personas fuera de los grupos de defensores de las libertades civiles se muestran en realidad preocupadas por su posible pérdida.

Lo anterior puede explicarse porque la vigilancia electrónica no ha tenido gran impacto en la vida de las personas, más allá de (por lo general) que facilita lidiar con la oficialidad. Pero con la recolección y la centralización de grandes cantidades de datos, el potencial de abuso es enorme y muy endebles los mecanismos de protección.

Ross Anderson, profesor de la Universidad de Cambridge en Inglaterra, ha comparado la actual situación con una "rana hervida", la cual no salta para escapar de una cacerola si el agua aumenta de temperatura poco a poco. Si la libertad se erosiona a paso lento, la gente se acostumbrará. Sin embargo, es posible que la invasión a la privacidad alcance su punto crítico e instigue una revuelta.

Si no hay muchas señales de revuelta en las democracias occidentales podría ser porque la mayoría de las personas cree que sus autoridades luchan contra el terrorismo y evitan abusar de la información en su poder. La perspectiva parece mucho más peligrosa en países como Rusia y China, que han adoptado tecnología capitalista y la revolución de la información sin haber exorcizado por completo el *ethos* de un Estado autoritario, donde los disidentes, por pacíficos que sean, son vigilados muy de cerca.

La era de la información posibilita la aparición de una anticuada dictadura recolectora de expedientes y datos basada en un monopolio de las comunicaciones. Pero hay que imaginar qué clase de Estado podría surgir si los mejores cerebros de una fuerza policiaca secreta –fuerza cuya cultura trata a todo disidente como peligroso– perfeccionan el arte de reunir y usar información en masivos bancos computarizados y no en pequeños y amarillentos papeles.

FUENTE: EIU

Traducción de textos: **Jorge Anaya**