Sociedad

La privacidad en la encrucijada

Simon Davies
Fundador de ***Privacy International***

Traducción: José Alfonso Accino

1. Las pruebas de ADN

Un edificio gris y anodino de oficinas en Edimburgo alberga actualmente uno de los más extraordinarios episodios de la antigua lucha entre la intimidad individual y el poder del Estado. Aquí, en la sede central de la *Lothian and Borders Police*, se está archivando sistemáticamente el **ADN** de la población local.

Durante los últimos dos años, cada persona arrestada o detenida por la policía de Edimburgo ha sido obligada a someterse a una prueba de ADN. Los delitos merecedores de esta práctica no se limitan a las categorías obvias de asesinato, violación o robo, sino que se extienden también a las infracciones de tráfico, hurtos en comercios y alteraciones del orden público tales como la *Breach of the Peace*.

En lo que respecta a la privacidad, la política seguida en Edimburgo reviste enorme trascendencia. La recogida y almacenamiento de ADN debe ser considerada, con toda seguridad, como una de las mayores invasiones de la intimidad personal pero, a pesar de ello, parece haberse asegurado un apoyo público sustancial. Un reciente sondeo de opinión sugiere que alrededor de las tres cuartas partes de la población local estaría dispuesta a facilitar su ADN en la «persecución de un crimen».

La policía se niega a reconocer que tales prácticas tengan consecuencias para los derechos civiles. Un portavoz de la policía manifestó recientemente a la **BBC**: «*Tenga en cuenta que la persona que comete una infracción de tráfico puede ser un delincuente de importancia y es nuestra oportunidad para recoger su ADN e identificarlo*».

Es aún demasiado pronto para hacerse una idea del éxito obtenido por tal programa, pero el Primer Ministro Tony Blair ya ha señalado que él quiere que todas las fuerzas de policía del Reino Unido sigan el ejemplo de Edimburgo. Si es así, es probable que dentro de una generación el ADN de la mayoría de la población del Reino Unido haya sido archivado en la base de datos nacional de ADN.

También el Ministerio del Interior y otras instituciones gubernamentales se han entusiasmado por el potencial de las pruebas de ADN. La legislación reciente de la *Child Support Agency* obliga a todos los que nieguen su paternidad a someterse a una prueba de ADN. La negativa a hacerlo así es legalmente equivalente a un reconocimiento de culpabilidad.

La actual obsesión por las pruebas de ADN apunta directamente al centro de la cuestión de la privacidad. Tradicionalmente, la invasión de la intimidad se ha justificado sobre la base de un gobierno efectivo de la sociedad. La policía ha argumentado siempre que la privacidad y el anonimato son malas noticias para la aplicación de la ley. Las autoridades siempre se ha esforzado por conseguir una perfecta identificación de los ciudadanos. Y el ADN es el identificador perfecto.

2. El individuo y el Estado

Pero la popularidad de las pruebas de ADN es meramente un síntoma de una tendencia mucho más amplia en todo el mundo. Gobiernos y organizaciones del sector privado han ido avanzando en años recientes hacia la inclusión de la vigilancia en casi todos los aspectos de nuestras finanzas, comunicaciones y forma de vida. Mientras se alaba la privacidad de boca para fuera, se argumenta que la vigilancia es necesaria para mantener la ley y el orden y para conseguir eficacia económica. La justificación es a menudo interesada y algo falsa, pero una cantidad sustancial de personas han sido persuadidas, no obstante, de que la renuncia a la intimidad es el precio que hay que pagar por una sociedad mejor y más segura.

La cuestión no ha sido nunca sencilla. La protección de la privacidad individual ha sido siempre una de las grandes polémicas de los derechos humanos. En su centro se encuentra la lucha por encontrar el equilibro ideal entre la autonomía del individuo y el poder del Estado.

Esta lucha por el equilibrio se desarrolla cada día de mil maneras. Con cada nueva intromisión en la vida privada --ya sea Televisión en Circuito Cerrado (TVCC), vigilancia del correo electrónico o publicidad directa-- la gente se ve obligada a elegir entre sus derechos individuales y los derechos de la sociedad.

Sin embargo, aunque el problema --hay que admitirlo-- es más complejo de lo que lo ha sido jamás, también es más acuciante que nunca. Probablemente, nunca ha habido un momento en la historia en el que se haya acumulado tanta información sobre la población en general. Los detalles de un adulto medio económicamente activo, del mundo desarrollado, se encuentran en cerca de 400 de las principales bases de datos: suficiente información procesada como para recopilar un enorme historial de cada persona. La vigilancia

visual electrónica en los centros urbanos es ya omnipresente. Casi todas las formas de comunicación electrónica se exploran y analizan ya rutinariamente.

Estas actividades han dado lugar a un sector económico floreciente. En Gran Bretaña, la industria de vigilancia en todas sus formas --investigadores privados, agencias de crédito, servicios de seguridad, etc.-- emplea a más de un millón de personas. Tal población de fisgones profesionales se explica, en parte, por la aparición de la vigilancia de masas. En el pasado, la vigilancia apuntaba a individuos o grupos específicos. Ahora, la vigilancia sistemática en un número creciente de ámbitos analiza activamente a millones de personas a la vez.

Tradicionalmente, la reacción pública a la invasión de la intimidad ha sido contradictoria e impredecible. Aunque las encuestas de opinión muestran consistentemente que la gente se preocupa por la intimidad, la oposición pública, incluso a la más descarada invasión de la privacidad, es escasa.

En los Estados Unidos, la toma de huellas digitales a los perceptores de la beneficencia social ha proseguido con un escaso murmullo de protesta mientras que, en Australia, los intentos del gobierno federal de introducir una tarjeta nacional de identidad provocaron en los años ochenta las mayores protestas públicas que se recuerdan en ese país. Sin embargo, mientras la legislación australiana que obliga a los bancos a informar de las transacciones sospechosas pasó sin llamar la atención, leyes similares en los Estados Unidos provocaron más de un cuarto de millón de quejas por escrito.

En Alemania y Australia, las propuestas de introducir servicios de telefonía digital desataron un amplia preocupación por la intimidad. Idéntica tecnología fue introducida en Gran Bretaña con escasa o nula discusión.

3. La privacidad como derecho humano

Causa o efecto, la privacidad ocupa ahora un lugar poco envidiable en el catálogo de los derechos humanos. Junto a la censura y la libertad de expresión, la privacidad sigue siendo una polémica compleja, y su solución un desafío. Durante el último cuarto de siglo, ningún otro derecho fundamental en el ámbito de la política pública ha generado tanta turbulencia y controversia. Y sin embargo, como un escritor ha observado, «la privacidad es el derecho del cual todos los demás se derivan». Es el centro de la libertad y autonomía del pueblo y es, tal vez, el factor clave que limita el poder del Estado.

Tortura, discriminación, odio racial: todas estas cuestiones han conseguido un consenso básico en la comunidad internacional. La privacidad, sin embargo, es percibida por muchos gobiernos y corporaciones como el «coco» de los derechos humanos. Es un lugar común para muchas organizaciones el que la privacidad y la protección de la información personal impiden el rendimiento económico y la aplicación de las leyes. El resultado es que muchos países se están convirtiendo en sociedades vigiladas. La justificación es seductora y difícil de contrarrestar (los habitantes de Edimburgo saben todo ésto demasiado bien). Y en nuestro inocente y natural deseo de ahorrarnos unos pocos dólares, o simplemente de ser buenos ciudadanos, cedemos constantemente información acerca de nuestras finanzas, compras, empleo, intereses, actividad telefónica, e incluso nuestros desplazamientos geográficos. Inevitablemente, cuando así lo hacemos, las organizaciones están listas para explotar esos datos. La vigilancia se ha convertido en un componente fijo de la próspera economía de la información.

Es ya un lugar común que la potencia, capacidad y velocidad de la tecnología de la información se están acelerando rápidamente. El alcance de la invasión de la privacidad --o al menos el potencial para invadirla-- crece a la par. Pero no es sólo la acrecentada capacidad y el costo decreciente de la tecnología de la información lo que genera amenazas a la privacidad. La globalización de sistemas como Internet elimina las limitaciones geográficas (y las protecciones legales) al flujo de los datos. La convergencia está conduciendo a la eliminación de las barreras tecnológicas entre sistemas. Los modernos sistemas de información tienen una creciente capacidad de interacción con otros sistemas y pueden intercambiar mutuamente y procesar diferentes clases de datos. Entretanto, el fenómeno multimedia, que funde varias formas de transmisión y expresión de datos e imágenes, crea enormes dificultades a los legisladores que desean proteger la intimidad personal.

Recientemente, presenté en la cadena de **TV BBC2** un documental sobre la privacidad, en el que describía uno de los resultados imprevistos de estas macro-tendencias de la tecnología: una compañía, *UK InfoDisc*, ha producido un CD-ROM que cruza los datos de las listas electorales con los de la guía telefónica y datos geodemográficos. Así, la más elemental e inocente información acerca de usted puede ser introducida en el disco, revelando toda clase de hechos. Su número de teléfono lleva instantáneamente a su dirección. Su nombre lleva automáticamente a su profesión y edad. No es necesario decir que los sectores de finanzas y créditos, investigadores privados, periódicos, empresas de mercadotecnia y policía hacen uso intensivo de este producto.

Estas cuestiones son importantes porque el creciente lazo de información entre el ciudadano y el Estado (y el sector privado, naturalmente) disminuye la autonomía humana. Conforme se automatiza la toma de decisiones por las instituciones, los factores que afectan a nuestras vidas se construyen sobre la base de una masa creciente de datos personales íntimos. El riesgo de desarraigo o discriminación se intensifica paralelamente.

4. Los países en vías de desarrollo

En los países en vías desarrollo, la amenaza es aún mayor. La perfecta identificación de los individuos puede tener fatales consecuencias. Los gobiernos de las naciones en desarrollo confían en que los países del primer mundo los equipen con tecnologías de vigilancia como equipos de intervención telefónica digital, equipos de descifrado,

escáners, escuchas, equipos de seguimiento y sistemas de intervención en ordenadores. La transferencia de tecnología de vigilancia desde el primer al tercer mundo es ahora un lucrativo negocio suplementario para la industria de armamento. Un informe publicado en 1995 por mi organización destacaba el alcance de este comercio[1].

Esta visión fué corroborada por el informe de 1997, «Evaluación de las Tecnologías de Control Político», encargado por el Comité de Libertades Civiles del Parlamento Europeo, y llevado a cabo por la Oficina de Evaluación de Opciones en Ciencia y Tecnología (**STOA**) de la Comisión Europea[2].

El comercio internacional en tecnología de vigilancia (algunas veces conocido como el Comercio de la Represión) implica la fabricación y exportación de tecnologías de control político. Estas tecnologías incluyen una sofisticada tecnología informática que amplía enormemente el poder de las autoridades.

El informe de Privacidad Internacional listaba las compañías que exportan dicha tecnología a países en desarrollo con un escaso historial de derechos humanos. Los intentos realizados, tanto por el informe del Parlamento Europeo como por Privacidad Internacional, por aumentar el grado de conciencia acerca de las implicaciones éticas de la transferencia de tal tecnología, se han visto acrecentados por informes recientes de Amnistía Internacional, *Human Rights Watch* y *Oxfam*. La imagen es convincente: «*El comercio de vigilancia es casi indistinguible del comercio de armas. Más de un setenta por ciento de las compañías que fabrican y exportan tecnología de vigilancia también exportan armas convencionales, químicas o equipo militar. La vigilancia es un elemento crucial para el mantenimiento de cualquier infraestructura no democrática y una actividad importante en la consecución del control político y de inteligencia. Muchos países en transición a la democracia también confían ampliamente en la vigilancia para satisfacer las demandas de la policía y los militares*»[3].

Según el informe STOA, gran parte de esta tecnología se utiliza para seguir las actividades de disidentes, activistas de derechos humanos, periodistas, líderes estudiantiles, de minorías o sindicales, y opositores políticos. Los sistemas de identificación a gran escala son también útiles para monitorizar grandes sectores de la población. Como señalaba *Privacy International*, «*en ausencia de un significado legal o protecciones constitucionales, tal tecnología es lo opuesto a una reforma democrática. Puede, ciertamente, resultar fatal para cualquiera persona 'de interés' para un régimen*».

5. Las tecnologías de vigilancia

La visión de que la tecnología de vigilancia es inherentemente hostil a los derechos individuales fue expuesta con cierta vehemencia en el informe STOA de 1997 [4]. El informe sitúa varias categorías de tecnologías de la información --sistemas de ifentificación, tecnología biométrica, sistemas de intervención telefónica, etc.-- bajo una luz negativa, vinculando su realización a la denegación de derechos humanos básicos. El informe concluye que tales tecnologías (que describe como «nueva tecnología de vigilancia») pueden ejercer un poderoso efecto disuasorio sobre todos aquellos que «*pudieran tomar un punto de vista disidente y pocos se arriesgarán a ejercer su derecho a una protesta democrática*». Estos factores se hallan también presentes en el incipiente debate sobre el uso por el Estado de la Televisión en Circuito Cerrado (**TVCC**).

El informe también pone de relieve el uso hostil que esta tecnología podría recibir en distintos regímenes, y las implicaciones éticas derivadas de la exportación de dicha tecnología a esos países.

Mientras que las compañías de **TI** presentan rutinariamente sus tecnologías como una manera de lograr una reforma de la sociedad, los defensores de los derechos humanos las definen como un medio de control social y político.

Este control será mucho más evidente en los años venideros. Hacia el 2020, de seguir las actuales tendencias, es probable que el alcance de la invasión de la intimidad sea absoluto.

La TVCC puede resultar la más obvia --y onerosa-- de las intromisiones futuras. En Gran Bretaña, se han colocado cientos de miles de cámaras en autobuses, trenes, ascensores e incluso cabinas telefónicas. Mucha gente ahora da por hecho que será filmada desde el momento en que sale por la puerta. Cámaras ocultas, antes objeto de desaprobación, están siendo instaladas ahora sin más problemas en cines, cascos de policías, bares, zonas de alterne, vestuarios y bloques de viviendas. Considerada hace tiempo como una indisimulada herramienta de vigilancia, tras un plazo de quince años la TVCC es ahora percibida como una parte integral y benigna del entorno urbano.

Olvide por un momento la engorrosa tecnología representada en *1984*. Es la integración de la vigilancia con el entorno lo que la hace más eficaz.

En Gran Bretaña, la vigilancia visual se está convirtiendo en un componente fijo del diseño de los modernos centros urbanos, nuevas áreas de viviendas, edificios públicos e incluso a través de la red de carreteras (una red masiva de cámaras, conectadas, para la identificación de matrículas terminarán con el anonimato en la carretera de aquí a diez años). Pronto, la gente esperará que la tecnología de espionaje se integre en todas las formas de arquitectura y diseño. Es, tal vez, sólo una cuestión de tiempo antes de que las presiones legales y colectivas introduzcan las cámaras en nuestras casas.

6. ENFOPOL, ECHELON, SORM ....

La omnipresencia de la vigilancia visual tendrá su paralelo en la vigilancia en masa de la actividad telefónica y de Internet. Las instituciones de seguridad de Europa y Estados Unidos han puesto ya los cimientos para un sistema de

escucha masiva capaz de interceptar los teléfonos móviles, las comunicaciones por Internet, los mensajes de fax y buscapersonas a través de toda Europa.

El plan, conocido como **ENFOPOL 98**, ha sido llevado en secreto por funcionarios de Policía y Justicia, como parte de una estrategia paneuropea para crear una red sin fisuras para la vigilancia de las telecomunicaciones por encima de las fronteras nacionales.

La estrategia, que ha recibido un amplio apoyo del Consejo de Justicia e Interior de la UE --máximo servicio policial de Europa-- obligará a todos los proveedores de servicios Internet e intercambios telefónicos a dar a las instituciones acceso «en tiempo real y a tiempo completo» a todas las comunicaciones, independientemente del país de origen. Todos los nuevos medios de comunicación, incluyendo la televisión interactiva por cable, serán también obligados a dar pleno acceso a las fuerzas de seguridad.

El sistema ENFOPOL se ayudará de un sistema de «etiquetado de un sujeto» capaz de seguir la pista de un individuo a cualquier lugar que vaya. Conocido como *International User Requirements for Interception* (**IUR**), el sistema de etiquetado, que está siendo desarrollado actualmente, creará una red de transmisión y proceso de datos que incluirá no sólo nombres, direcciones y números de teléfono de los «objetivos» y sus asociados, sino direcciones de correo electrónico, detalles de tarjetas de crédito, *PINs* y contraseñas.

El sistema cruzará además los datos de teléfonos móviles para crear un sistema exhaustivo de seguimiento de localización geográfica.

ENFOPOL es sólo uno entre los varios sistemas que están surgiendo para rastrear y analizar las comunicaciones internacionales. Tal vez el más sorprendente sea **ECHELON**, un sistema global de escucha establecido por la Agencia Nacional de Seguridad de los Estados Unidos. Este sistema fue diseñado para operar en el núcleo de los sistemas internacionales de telecomunicaciones y puede escudriñar decenas de millones de mensajes de correo y faxes para descubrir palabras de interés para los Estados Unidos y sus aliados.

En el Reino Unido, el proyecto de ley de Regulación de Poderes de Investigación (conocido en Rusia como Ley SORM), en su tercera revisión por hoy, proporcionará al gobierno un arsenal de poderes para poner los ordenadores e Internet bajo vigilancia. Las medidas tienen el efecto potencial de criminalizar a los usuarios de sistemas de cifrado (y ésto, en última instancia, significa cualquier futuro usuario de ordenadores). El proyecto también da a casi todas las autoridades el derecho, sin necesidad de mandamiento judicial, de supervisar la información sobre el tráfico de Internet. Esto es, qué sitios web se ha visitado, a quién se ha enviado correo electrónico o qué grupos de noticias se leen.

Las autoridades fiscales usarán la ley en el futuro para dirigir una masiva operación de captura por toda la Internet, analizando y elaborando perfiles sobre las actividades de millones de usuarios.

Una vigilancia perfecta requiere una no menos perfecta identificación y los próximos veinte años verán un exhaustivo esfuerzo de las autoridades para conseguir este fin. Además de establecer el uso extensivo de pruebas de ADN para distintos propósitos, es probable que administraciones públicas y empresas introduzcan un sistema nacional de huellas digitales electrónicas y escáners de mano.

Estos sistemas, conocidos como «identificadores electrónicos», están ya en uso en todo el mundo. Según afirman, obtienen una identificación casi perfecta del individuo escaneando los más finos detalles de una mano, un dedo o un ojo.

Diversos planes de biometría están siendo llevados a cabo por todo el mundo. España ha comenzado un sistema nacional de huellas digitales para los beneficiarios del desempleo y la seguridad social. Rusia ha anunciado sus planes para un sistema nacional de huellas digitales electrónicas para los bancos. Los jamaicanos están obligados a escanear sus pulgares en una base de datos antes de ser autorizados a votar en las elecciones. En Francia y Alemania se están probando equipos que permitan incluir huellas digitales en las tarjetas de crédito. Esta tecnología está siendo utilizada por concesionarios, guarderías, fuerzas de seguridad y cajeros automáticos. *Microsoft* anunció recientemente que tiene intención de incorporar biometría en sus nuevos sistemas operativos para ayudar a la seguridad en Internet.

Durante los últimos cinco años, el Servicio de Inmigración y Naturalización de los Estados Unidos (**INS**), o «Migra» como la denominan los hispanos, ha estado desarrollando un sistema automático de control de pasaportes utilizando la geometría de la mano. En este proyecto, los viajeros habituales tienen su geometría manual almacenada en una tarjeta inteligente. El viajero coloca una mano en un escáner e inserta su tarjeta en una ranura. Más de setenta mil personas han participado en la prueba. Un portavoz del INS informó reciente al *Daily Telegraph* que la organización pretende crear un sistema biométrico para viajeros de amplitud mundial.

7. Vigilancia en el puesto de trabajo

Pero será el incremento de la vigilancia en el puesto de trabajo lo que afectará más directamente a la gente. En la mayoría de los países, los trabajadores casi no tienen derecho a la privacidad. Los empresarios tienen permiso --«justificado»-- para poner a todos los empleados bajo constante vigilancia. Pueden intervenir los teléfonos, leer el correo electrónico y controlar las pantallas de los ordenadores. Pueden escuchar las conversaciones, analizar el comportamiento del ordenador y del teclado, curiosear mediante cámaras de TVCC, utilizar tecnología de seguimiento para controlar los movimientos personales, analizar la orina para detectar el uso de drogas y exigir la revelación de datos personales íntimos. La

creciente precariedad de la fuerza de trabajo acelera todas estas actividades.

Software telefónico como *WatchCall*, de *Harlequin*, analiza los números de las llamadas que los empleados realizan y reciben. En las industrias basadas en el ordenador y el teléfono, tales programas han convertido a los supervisores en el equivalente digital de los capataces de los asilos victorianos para indigentes. La nueva generación de tecnología de supervisión es extremadamente efectiva. Puede analizar las pulsaciones en un teclado para determinar si los empleados usan eficientemente su tiempo entre conversaciones telefónicas.

Incluso los trabajadores altamente cualificados pueden esperar ser puestos de forma habitual «bajo el microscopio». Es probable que cualquier director que adquiere un software de sistema operativo de red reciba al mismo tiempo funciones, ya incluidas, de escucha. Algunos paquetes como *Win Watch Professional* y *Norton Lambert's Close-Up/LAN*, permiten a los administradores de la red observar las pantallas de los empleados en tiempo real, explorar los archivos de datos y el correo electrónico, analizar las pulsaciones del teclado e incluso saltarse las contraseñas.

Estas tendencias sólo pueden tener un resultado: el puesto de trabajo del mañana tendrá muchas de las características de los asilos de indigentes descritos por Dickens.

8. Vigilancia en el hogar

Incluso su hogar no estará a salvo de la vigilancia. Considere la nueva generación de servicios de televisión digital interactiva. Estos productos ofrecen una nueva familiaridad entre el proveedor de servicios de TV y el cliente. Extrayendo directamente la información de los hábitos televisivos del cliente, transacciones financieras y encuestas «en pantalla», la compañía puede crear un perfil complejo de cada cliente.

Un nuevo libro *Spy TV* (La televisión espía) del investigador estadounidense David Burke explica cómo el nuevo sistema invade subrepticiamente la privacidad de los clientes. Burke ha incluído algunas citas literales de entusiasmados directores de mercadotecnia. En palabras del jefe de *Procter&Gamble*, Edmin Artzt, quieren «*hincarle el diente a toda esta nueva tecnología y convertirla en una época de bonanza para la publicidad*».

La televisión interactiva (también conocida como i-TV) va mucho más allá de la publicidad, ya que promete --según la apreciación del analista de información del Reino Unido, William Heath-- «*crear unas condiciones experimentales totales en el hogar de cada usuario, con un ciclo mensurable de estímulos, medida y respuesta*».

«*Podemos elaborar perfiles de la gente... En último término, el producto se dirigirá por sí mismo a los clientes individuales*», dice Simon Cornwell, de *Two Way TV*. «*La gente revela muchísmo acerca de sí misma*», dice Nick Bryant, de *BiB*. «*Es publicidad despersonalizada*», dice Howard Hughes, de *NTL*: «*Con los datos que nos llegan de vuelta, recordaremos todo acerca de cada uno*». Pat Dade, de *Synergy Consulting* cree incluso que los incomprendidos consumidores de hoy recibirán con agrado la posibilidad de ser psicoanalizados a través de sus propios televisores.

Como Heath ha señalado, «*No es que los consumidores lo estén reclamando clamorosamente, pero los promotores pueden ver que les puede hacer ganar más dinero que Internet. Es como un promotor inmobiliario mirando el éxito de Portobello Road e intentando entusiasmar al mundo acerca de su nuevo proyecto de centro comercial que viene completo con TVCC y tarjetas de fidelidad*».

9. Notas

[1] *Big Brother Incorporated*, *Privacy International*. *www.privacy.org/pi/*
[2] STOA. Ref: proyecto n. IV/STOA/RSCH/LP/politicon.1
[3] *Big Brother Incorporated*
[4] STOA. Ref: proyecto n. IV/STOA/RSCH/LP/politicon.1