

# *Un Informe sobre la sociedad de la vigilancia*

Para el Comisario de información  
elaborado por la Red de Estudios sobre Vigilancia

## *Documento de debate público*

Septiembre de 2006

Editado por:

David Murakami Wood y Kirstie Ball

Basado en contribuciones de:

Louise Amoore  
Kirstie Ball  
Steve Graham  
Nicola Green  
David Lyon  
David Murakami Wood  
Clive Norris  
Jason Pridmore  
Charles Raab  
Ann Rudinow Saetnan

### **Londres 2016: todo está bajo control<sup>1</sup>**

Mientras el joven de 18 años Ben Jones y sus compañeros de la manifestación en contra de la guerra caminan por el centro de Londres se encuentran bajo supervisión constante. Pequeños vehículos aéreos no pilotados (en inglés, UAV – Unmanned Air Vehicles) teledirigidos vuelan en círculos sobre sus cabezas<sup>2</sup>. Estos aviones espía se introdujeron en los juegos olímpicos de 2012 y el “éxito” de lo que la publicidad ha dado en llamar “ojos voladores amigos en el cielo” ha sido defendido por el alcalde como el motivo para continuar usándolos<sup>3</sup>. Ahora la gente ya casi ni se da cuenta de que están ahí. Pequeñas cámaras integradas en las farolas y los muros a la altura de los ojos así como más arriba permiten un funcionamiento más eficaz de los sistemas de reconocimiento facial que ahora son universales<sup>4</sup>. También se están desarrollando programas de software morfológico que combinan imágenes de múltiples cámaras para formar imágenes tridimensionales, aunque sus detractores y los abogados argumentan que es impreciso y que no constituye una imagen “real”. Las ya casi universales redes inalámbricas permiten eliminar las grandes cajas y cables de las cámaras. Además, están conectadas a una iluminación callejera inteligente que proporciona unas condiciones de iluminación “ideales” para el reconocimiento facial así como para los reflectores automáticos y para las cámaras adicionales que se activan mediante movimientos “sospechosos”. Numerosos edificios estatales importantes que permanecían rodeados de barricadas de cemento desde 2001 ahora parecen volver a abrirse, aunque en su lugar están protegidos por una serie de sensores conectados a barricadas automatizadas e impenetrables que se hunden en el pavimento cuando no se necesitan de inmediato.

Al regresar hacia el metro, Ben y su amigo Aaron se pierden accidentalmente y entran en la Zona de exclusión de Westminster. Les detiene el personal de seguridad privado contratado por el Distrito de mejora empresarial (Business Improvement District, BID)<sup>5</sup> de Westminster. Este personal está supervisado de forma remota por los operadores de policía, mediante sus ordenadores de mano<sup>6</sup> y las microcámaras integradas en los cascos protectores, con las que escanean a los dos muchachos<sup>7</sup>. Ben se somete a la toma de muestras de ADN habituales, que se analizan de forma instantánea, y entrega su carné de identidad, para pasarlo por el identificador. Al aparecer la información en la pantalla, el agente bromea diciendo que es irónico que un anticapitalista como él acabe de volver de unas vacaciones en los EE.UU.<sup>8</sup> Ben hace una mueca cortés. Se supone que los carnés de identidad son todavía voluntarios y Aaron, que proviene de una familia de profundas raíces cristianas, se niega a tener uno. Su madre dice que es la “marca de la bestia”, pero él sólo quiere que le dejen en paz. Sin embargo, ahora esto le está resultando difícil: el no tener carné de identidad significa que no tiene opciones reales a solicitar puestos estatales ni a recibir prestaciones ni préstamos de estudiante, ni tampoco puede viajar en avión ni en tren, incluso dentro de Gran Bretaña. Empieza a preguntarse si vale la pena y cómo logrará sobrevivir. Las cosas están a punto de empeorar para él: al ser un joven varón y negro sin carné de identidad, está clasificado con un nivel de riesgo alto en los perfiles de la policía por lo que la central solicita al personal de seguridad que lo lleven a la comisaría para interrogarlo más detenidamente<sup>9</sup>...

Este 2016 imaginario no está tan lejos.

En 2004, el Comisario de Información, Richard Thomas, el agente designado por el Parlamento para actuar como organismo de control en el uso de nuestros datos personales, advirtió que estamos “entrando a ciegas en una sociedad de vigilancia”<sup>10</sup>.

Pero, en realidad, ya vivimos en una sociedad vigilada:

- Las cámaras de vídeo nos vigilan a dondequiera que vayamos: edificios, calles con tiendas, carreteras y áreas residenciales. Los sistemas automáticos actuales pueden reconocer matrículas (y, cada vez más, rostros).
- Los transmisores electrónicos garantizan que las personas en libertad condicional no violan sus condiciones de libertad. La policía toma muestras de ADN de las personas arrestadas, las cuales se archivan ya sean declaradas culpables o no. Cada vez se están identificando “tendencias criminales” más pronto en la vida de una persona.
- Constantemente se nos pide que probemos nuestra identidad para obtener prestaciones de asistencia social, asistencia sanitaria, etc. El gobierno del Reino Unido tiene previsto introducir un nuevo sistema de carnés de identidad biométricos que incluyen datos biométricos (huellas dactilares y reconocimiento de iris) vinculados a una inmensa base de datos de información personal.
- Cuando viajamos al extranjero, se comprueba y realiza un seguimiento de nuestra identidad, nuestro destino y nuestro equipaje, y estos datos son almacenados. Nuestros pasaportes están cambiando y ahora cuentan con chips informáticos que almacenan información, y al igual que ocurren con los carnés de identidad, existen propuestas para emitir pasaportes biométricos.
- Un gran número de escuelas utilizan tarjetas inteligentes (e incluso técnicas biométricas) para supervisar dónde se encuentran los niños, qué comen o los libros que sacan de la biblioteca.
- Programas de software analizan nuestros hábitos de compra y esos datos son vendidos a todo tipo de empresas. Cuando llamamos a centros de llamadas o solicitamos préstamos, seguros o hipotecas, la rapidez con la que obtenemos estos servicios y los artículos que nos ofrecen dependen de lo que gastamos, dónde vivimos y quiénes somos.
- Los servicios de inteligencia británicos y estadounidenses pueden interceptar nuestros teléfonos, correos electrónicos y el uso que hacemos de Internet para buscar palabras y expresiones clave.
- Cada vez se nos controla más de cerca en el trabajo para determinar nuestro rendimiento y productividad, y las organizaciones para las que trabajamos están empezando incluso a estudiar nuestras actitudes y estilo de vida fuera del lugar de trabajo<sup>11</sup>.

La sociedad de la vigilancia ha llegado sin que casi nos hayamos dado cuenta.

Es el resultado final de numerosos cambios tecnológicos diferentes, incontables decisiones políticas y diversos avances sociales. En parte, resulta esencial para facilitar los servicios que necesitamos: salud, prestaciones, educación. En parte, resulta cuestionable. En parte, puede resultar injustificable, intrusiva y opresiva. Es posible que la gente tenga opiniones variadas al respecto. Pero, de hecho, la mayoría de la gente sabe muy poco sobre la sociedad de la vigilancia: se percibe como historias de ciencia ficción, no de la vida cotidiana. Y, en consecuencia, se ha generado muy poco debate público sobre la misma. La industria de la vigilancia ya alcanza proporciones inmensas (particularmente desde el 11-S) y está creciendo muchísimo más rápido que el resto de los sectores<sup>12</sup>: se calcula que globalmente su valor es de aproximadamente 1 trillón de dólares estadounidenses y abarca una inmensa gama de bienes y servicios, desde equipamiento militar, pasando por las cámaras de CCTV en las calles comerciales, hasta las tarjetas inteligentes. La sociedad de la vigilancia con frecuencia se ha introducido de forma lenta, sutil e imperceptible y

mediante una combinación imprevista de numerosas pequeñas rutas se ha abierto camino hasta una calle más grande. Se trata de una calle cuya dirección debemos analizar y debatir de forma urgente.

### ***Cuidando de ti***

Geeta tiene 69 años y vive sola en su piso. Además de los detectores de movimiento de emergencia, la bañera dispone de un monitor de ritmo cardíaco integrado, la taza del inodoro tiene un dispositivo que mide su nivel de azúcar en sangre, y la cocina cuenta con una serie de sensores para detectar fugas de gas, incendios e inundaciones. Geeta también dispone de un botón de emergencia conectado con el centro telefónico de la autoridad local, desde donde pueden llamarla inmediatamente para comprobar cómo se encuentra, en caso de haberlo pulsado. La presencia de sensores y cámaras por toda la casa significa que su familia sabe que se encuentra segura y como resultado recibe menos visitas familiares que antes, lo que hace que se sienta un poco aislada. No obstante, los detectores de RFID (identificación por radiofrecuencia) en su frigorífico y alacenas le resultan de gran utilidad: cada vez que se le agotan los comestibles, el ordenador de administración para el hogar envía por Internet un pedido automático a su supermercado local. Al estar suscrita a las entregas domiciliarias no necesita ir a las tiendas innecesariamente. También está acostumbrada a sus habituales chequeos “Mujer saludable”. Sin embargo, sin que ella lo sepa, el Servicio de salud británico (NHS) compara los resultados de Geeta con los de otras mujeres de su misma edad en todas las regiones de las autoridades sanitarias del país<sup>13</sup>. Esto les permite tomar decisiones sobre los factores de riesgo para, por ejemplo, poder predecir un ataque al corazón con un grado de precisión mucho más alto. En consecuencia, Geeta recibe recomendaciones dietéticas ya que se encuentra en un grupo con riesgo alto de problemas vasculares. Pero existen otros problemas: en la actualidad el servicio de salud británico está evitando grandes ofertas económicas de agencias de seguros que desean acceder a información sanitaria sobre casos puntuales. Con unos recursos exiguos, estas ofertas resultan cada vez más tentadoras, aunque por el momento los directivos del servicio sanitario todavía se muestran reacios debido a un escándalo similar en Islandia, que entregó la totalidad de su base de datos de ADN a empresas privadas para realizar tareas de investigación así como para obtener beneficios a nivel privado.<sup>14</sup>

### **¿Qué tiene de malo una sociedad de vigilancia?**

La vigilancia no es una conspiración perversa urdida por poderes malignos. Una gran parte de la vigilancia tiene intenciones positivas o, al menos, neutrales: el deseo de seguridad, bienestar, salud, eficacia, rapidez y coordinación. Algunos tipos de vigilancia tienen como finalidad intencional limitar y controlar nuestro comportamiento o movimientos, a menudo sin nuestro conocimiento ni consentimiento. Y algunos tipos de vigilancia tienen este efecto sin pretenderlo. No obstante, esto no significa que todo ello resulte aceptable: resulta crucial comprender los efectos de la vigilancia y el impacto que ésta tiene en nuestra vida privada y en la sociedad.

Cada vez nos preocupamos más de los riesgos y peligros que de los objetivos sociales positivos que se desean obtener. A medida que más y más situaciones cotidianas se valoran en términos de “riesgo”, lo que antes suponía una seguridad excepcional se convierte ahora en normal. Sin embargo, casi nunca pensamos en las consecuencias no intencionadas que conducen a desigualdades de acceso y de oportunidades ni en las diferencias de clase, raza, género, geográficas y de ciudadanía que no sólo se agravan sino que además se convierten en intrínsecas al modo en que se toman todas las decisiones cotidianas.

Los procesos y las prácticas de vigilancia también contribuyen a crear un mundo en el que sabemos que no se confía verdaderamente en nosotros. La vigilancia fomenta la sospecha<sup>15</sup>. El empresario que instala monitores de pulsaciones de teclas en las estaciones de trabajo o dispositivos GPS en sus vehículos de servicio nos revela que no se fía de sus empleados. El administrador de prestaciones de asistencia social que busca pruebas de solicitudes dobles ilícitas de asistencia económica o pide información sobre “parejas que cohabitan” nos está diciendo que no confía en sus clientes. Y cuando los padres empiezan a utilizar cámaras web y sistemas GPS para vigilar las actividades de sus hijos adolescentes, también dejan de manifiesto que no confían en ellos.

La pregunta definitiva para la sociedad de la vigilancia es si estamos tan hipnotizados por la “necesidad” de encontrar soluciones de alta tecnología contra la delincuencia, el terrorismo, el fraude y numerosos otros problemas, que nos hemos olvidado de preguntarnos si esas soluciones son apropiadas y si es posible que haya otras respuestas no tecnológicas o menos invasivas.

Este breve documento y el informe completo que lo acompaña, han sido diseñados para comenzar a tratar estas cuestiones, para inspirar un debate público muy necesario. Es posible que deseemos vivir en una sociedad de vigilancia pero, aunque sea así, debe ser algo que decidamos con los ojos bien abiertos y con plena consciencia. En las siguientes páginas se describe en más detalle la sociedad de la vigilancia y sus consecuencias.

## ¿Qué es la sociedad de vigilancia?

La sociedad de la vigilancia es una sociedad que se organiza y estructura a través del uso de técnicas de vigilancia. Ser vigilado quiere decir que las tecnologías, en representación de las organizaciones y gobiernos que estructuran nuestra sociedad, están registrando información sobre nuestros movimientos y actividades. A continuación, esta información se clasifica, estudia y cataloga, y se utiliza como una base para tomar decisiones que afectan a las oportunidades y posibilidades de nuestra vida. Estas decisiones están relacionadas con nuestros derechos y con nuestro acceso a prestaciones de asistencia social, trabajo, productos, servicios y la justicia penal; con nuestra salud y bienestar y nuestros movimientos a través de los espacios públicos y privados.

En las siguientes páginas se destacan algunas de las características claves de la sociedad de la vigilancia: tecnología, flujo de datos, convergencia; clasificación social; dependencia y fallos tecnológicos.

## Tecnología

Vale la pena recordar que la vigilancia ha sido importante a lo largo de la historia y que algunos de los regímenes más autoritarios, como el de la antigua Alemania del Este, se han basado en algo tan poco sofisticado como archivos de papel e informantes<sup>16</sup>. Pero las tecnologías avanzadas han cambiado la vigilancia. Las nuevas tecnologías de la vigilancia son más pequeñas y poderosas, permiten recabar, almacenar e interrelacionar así como operar de forma más inmediata muchas más clases de información. Este documento no espera abarcar todas y cada una de las tecnologías de la vigilancia ni tampoco todos y cada uno de los sectores en los que se usan las mismas, sino que está diseñado para mostrar algunos de los cambios fundamentales que se han producido en cinco áreas clave: las tecnologías de las bases de datos, telecomunicaciones, cámaras de CCTV, biométrica así como de control por medios electrónicos y de seguimiento.

### *Las bases de datos*

Los cimientos de todas las nuevas tecnologías de vigilancia son las bases de datos informáticas. Ahora es posible recopilar, tabular y establecer referencias cruzadas entre cantidades ingentes de

datos de forma mucho más rápida y precisa que con los viejos archivos de papel. Cantidades descomunales de datos personales sobre individuos normales y corrientes resultan fundamentales en la actualidad tanto para las empresas privadas como para los servicios públicos. Los diferentes conjuntos de datos se pueden contrastar entre sí para identificar a individuos y patrones de actividad sospechosos. También se pueden “minar” datos, es decir, analizarlos en gran detalle mediante tecnologías sofisticadas para revelar patrones que requieran una investigación más detallada.

Toda transacción proporciona un “rastreo de datos”, relacionable con un individuo o tipo de persona o lugar<sup>17</sup>. Estas transacciones incluyen el uso de tarjetas de crédito, tarjetas bancarias, teléfonos móviles, Internet, compras, búsquedas o llamadas telefónicas. Diariamente se generan datos adicionales mediante los programas de tarjetas de fidelidad, encuestas de clientes, grupos de sondeo, concursos promocionales, solicitudes de información sobre productos, contactos con los centros telefónicos, “cookies” de sitios web, foros de opinión de consumidores y transacciones de crédito. Con frecuencia, todo ello se encuentra revestido con datos de fuentes públicas como estadísticas nacionales y organizaciones sin ánimo de lucro o empresas especializadas en la obtención de datos, para crear “perfiles” de individuos o comunidades. Incluso las técnicas más sofisticadas llamadas Descubrimiento de conocimiento en bases de datos (Knowledge Discovery in Databases, KDD) ahora identifican patrones ocultos y predicen transacciones futuras de un modo cada vez más personal, por ejemplo, el modo en que *Amazon.com* ofrece a sus clientes libros y DVD que les puedan gustar<sup>18</sup>.

Las bases de datos son una parte clave del cambio en los servicios públicos, por ejemplo, el controvertido programa informático del Servicio nacional sanitario británico (National Health Service, NHS), *Connecting of Health (Conexión de la salud)*, el más grande de Europa<sup>19</sup>. Este programa conectará los archivos electrónicos de los pacientes (Electronic Patient Records, EPR) con información local para crear una base de datos digital nacional de todos los archivos médicos personales. Aproximadamente dos millones de personas son arrestadas cada año por la policía de Inglaterra y Gales. En la actualidad se toman muestras de huellas dactilares y de ADN a prácticamente todos los arrestados y éstas permanecen en las bases de datos policiales independientemente de su culpabilidad o inocencia. Existen cerca de seis millones de juegos de huellas dactilares en estas bases de datos<sup>20</sup> y la Base de datos nacional de ADN (National DNA Database), creada en 1995, actualmente contiene registros del ADN de 3,45 millones de individuos o, lo que es lo mismo, el 5,2% del total de la población. Hay que destacar que en la base de datos existe un perfil para el 40% de los varones negros en comparación con el 9% de varones blancos y un 13% de hombres asiáticos<sup>21</sup>. Otras bases de datos policiales incluyen el Sistema de reconocimiento automático de matrículas (Automatic Number Plate Recognition, ANPR), el Registro de delincuentes violentos y delincuentes sexuales (Violent Offender and Sex Offender Register, ViSOR) y una propuesta Base de datos nacional de imágenes faciales (Facial Images National Database, FIND). Está previsto que pronto todas estén conectadas entre sí mediante el Ordenador nacional del cuerpo de policía (Police National Computer, PNC)<sup>22</sup>, al que finalmente se podrá acceder no sólo en todas las comisarías sino que además, mediante el desarrollo de Airwave, el nuevo sistema de comunicaciones digital de la policía, también los agentes de patrulla en la calle podrán acceder a ellas mediante un ordenador de mano<sup>23</sup>.

Las fronteras nacionales se están convirtiendo en “fronteras inteligentes”, con ingentes bases de datos en el trasfondo que procesan información sobre los individuos y sus desplazamientos. Los perfiles se usan para crear listas de observación de pasajeros peligrosos o para identificar grupos que puedan entrañar un “nivel de riesgo más alto”. La creación manifiesta de perfiles raciales incluso se sugiere como una política oficial<sup>24</sup>.

### ***La vigilancia llega a casa***

Al regresar de sus vacaciones en Florida en 2016, la familia Jones se encuentra con una frontera bastante diferente. La gestión tanto de los servicios de inmigración como de los de control de fronteras de Gran Bretaña y de los EE.UU., junto con los de los países miembros de la UE y otros países G10 industrializados, se ha subcontratado al mismo consorcio privado transnacional, BorderGuard<sup>25</sup>. La amenaza continuada de la inmigración ilegal junto con la retórica gubernamental sobre la “guerra contra el terror” han llevado a esos gobiernos a aplicar un programa de “fronteras inteligentes”. El control de pasaportes consiste ahora en una serie de cámaras y escáneres que toman imágenes del rostro, iris y huellas dactilares. Éstas se comparan con las de los pasaportes biométricos estándar o, en el caso de Gran Bretaña con las del carné de identidad, introducidos en la totalidad de los países del G10 y de la UE<sup>26</sup>. La información en el chip RFID integrado ahora incluye los datos de ciudadanía, inmigración, visados y justicia penal junto con información sobre salud, la cual se compara instantáneamente con las bases de datos nacional e internacional, así como con una montaña de datos extraídos de transacciones comerciales que BorderGuard obtiene a través de empresas especializadas<sup>27</sup>. Para la mayor parte de la familia, el tránsito es rápido, pero para la abuela Geeta surgen problemas. Pakistán todavía no se ha sumado a la versión completa del programa de fronteras inteligentes y Geeta nunca ha obtenido un pasaporte biométrico. Por consiguiente, tiene que esperar en la fila durante horas y someterse a diversos cacheos y preguntas adicionales. A pesar de tener un carné de identidad británico, los rasgos claramente “asiáticos” de mamá Yasmin también suponen que su desplazamiento transfronterizo desencadena alarmas y preguntas adicionales. A continuación, en la aduana, se somete a todo el mundo a un escaneado corporal completo, un cacheo sin ropa virtual...<sup>28</sup>

### *Telecomunicaciones*

Las “telecomunicaciones” incluyen no sólo el viejo sistema telefónico de línea fija con llamadas de voz y fax, sino también teléfonos móviles (incluidos voz, texto, imágenes, sonidos e información dependiente de la ubicación) así como comunicaciones informáticas como Internet (“banda ancha”, etc.). En la época de los sistemas telefónicos analógicos gestionados por el estado, solía ser el caso de que los teléfonos eran “intervenidos” (generalmente, por la policía o los servicios de seguridad) para someterlos a vigilancia. Tres aspectos han cambiado: las propias tecnologías telefónicas (teléfonos móviles, fibra óptica, wi-fi, etc.), la combinación de telecomunicaciones y almacenamiento y procesamiento electrónico (correo electrónico, sitios web, etc.) y el cambio a empresas privadas de telecomunicaciones. Los cambios actuales suponen una creciente convergencia de tecnologías e “interoperabilidad”, es decir, diferentes tecnologías trabajando juntas.

Para que alguna de esas tecnologías “funcione” es necesario el intercambio de señales o datos entre diferentes dispositivos, así como que sea posible realizar un seguimiento de ese intercambio. Por ejemplo, se puede determinar la localización de los teléfonos móviles y los Proveedores de servicios de Internet (Internet Service Providers, ISP) pueden catalogar las visitas a los sitios web. A medida que las tecnologías de telecomunicaciones están más conectadas, se genera más información. La ley ahora requiere conservar esta información para su análisis: en febrero de 2006, los EE.UU. y el Ministerio del interior británico (Home Office) propusieron la conservación de los datos durante dos años a disposición de la policía para su examen.

Los países también filtran regularmente cantidades ingentes de tráfico telefónico, de télex, correo electrónico y fax por motivos de “interés nacional” (tanto intereses de seguridad como

económicos). Por ejemplo, el sistema denominado “ECHELON”, la red de vigilancia global operada por la Agencia de Seguridad Nacional (NSA) estadounidense, mantiene una enorme base en Menwith Hill, en North Yorkshire, donde filtra automáticamente de forma rutinaria todo el tráfico de telecomunicaciones que pasa a través del Reino Unido en busca de palabras y expresiones clave, y emplea cada vez más algoritmos sofisticados para el reconocimiento avanzado del habla e incluso del significado<sup>29</sup>.

### ***Vigilancia virtual***

Cuando la policía se lo permite, Ben se marcha, pero ahora su propio ordenador de mano<sup>30</sup> está sometido a seguimiento mediante el sistema Galileo<sup>31</sup>. También se le incluye en una lista de control de comunicaciones y su ISP recibe una orden automática de la segunda Ley regulatoria de poderes investigativos 2 de 2009 (RIP 2 Act 2009) para que todo su tráfico por Internet y comunicaciones de correo electrónico se archiven y se envíen a la policía<sup>32</sup>. Como la mayor parte de las comunicaciones telefónicas ahora se realizan a través de Internet (y las viejas líneas telefónicas fijas están desapareciendo), esto abarca la totalidad de las comunicaciones de Ben. Una de las consecuencias imprevistas del seguimiento de las comunicaciones de Ben es que su hermano pequeño, Toby, que ocasionalmente usa las cuentas de Ben (principalmente porque le encanta hacer cracking<sup>33</sup>), también es sometido a la vigilancia. Toby pasa la mayor parte de su tiempo en línea participando en juegos en línea masivos de multijugadores (Massively Multiplayer Online Games, MMOG), mundos virtuales que tienen sus propias normas y economías alternativas completas<sup>34</sup>. Sin embargo, incluso aquí ha penetrado la sociedad de la vigilancia. Estos mundos de datos y comportamientos de “avatares” en línea están controlados, particularmente por empresas, cuyo objetivo es descubrir nuevas oportunidades de mercados emergentes en la vida real, y en ellos hay una completa nueva clase de jugadores empresariales que sólo existen para investigar los hábitos de las personas mediante sus avatares y realizar un marketing viral tanto de productos virtuales como reales dentro y fuera de esos mundos a los jugadores<sup>35</sup>. La policía también ha comenzado a experimentar con aplicaciones de software que controlan mundos virtuales para identificar avatares que muestran ciertos tipos de comportamiento, los cuales podrían apuntar a tendencias criminales de sus jugadores en el mundo real<sup>36</sup>. Por supuesto, levanta grandes controversias entre los jugadores, que argumentan que el escapismo a los mundos virtuales no se debe confundir con la vida real.

### *La vigilancia por vídeo*

Aunque se remonta a la década de 1960, el periodo de crecimiento de los circuitos cerrados de televisión (CCTV) en el Reino Unido data de finales de la década de 1980, instigado por los intentos para invertir el declive de los distritos comerciales en el centro de las ciudades así como por temor al terrorismo, la delincuencia y el vandalismo. En la actualidad es probable que el número de cámaras de CCTV en Gran Bretaña se aproxime a 4,2 millones: una por cada 14 personas<sup>37</sup> y un mismo individuo puede ser filmado por más de 300 cámaras al día<sup>38</sup>. Se calcula que durante la última década<sup>39</sup> se han invertido unos 500 millones de libras esterlinas de dinero público en la infraestructura de cámaras de CCTV, aunque un estudio del Ministerio del interior británico llegó a la conclusión de que “los programas de cámaras de CCTV que se han evaluado han tenido un resultado general reducido sobre los niveles de delincuencia”<sup>40</sup>.

La digitalización ha permitido un incremento automático en el uso de sistemas de cámaras de CCTV. Se utilizan las matrículas de los vehículos para identificar al propietario registrado. El uso de cámaras para hacer cumplir las restricciones de velocidad se ha incrementado de 300.000 incidentes en 1996 a más de dos millones en 2004, con una recaudación aproximada de 113

millones de libras al año<sup>41</sup>. Este aumento en la vigilancia estatal ha recibido críticas sistemáticas en la prensa<sup>42</sup>, a pesar del hecho de que las cámaras de control de velocidad, a diferencia de las cámaras de CCTV ubicadas en las calles, han tenido un impacto significativo en la reducción de muertes y heridas causadas por accidentes de tráfico.<sup>43</sup>

Se prevé que la intensificación en la vigilancia de los motoristas crecerá rápidamente. En marzo de 2005, la Asociación de Jefes de Policía (Association of Chief Police Officers) exigió la introducción de una red nacional de lectores de matrículas que “utilice cámaras policiales, de las autoridades locales, de tráfico (Highways Agency) y otros sectores asociados y comerciales”<sup>44</sup>, incluida la integración de las cámaras existentes en el centro de las ciudades y en las calles comerciales<sup>45</sup>, con un centro nacional de reconocimiento automático de matrículas (National ANPR (Automatic Number Plate Recognition) Data Centre). Este centro tendría la capacidad operacional para procesar 35 millones de lecturas para la identificación de matrículas al día, la cual ascendería a 50 millones en 2008 y cuyos datos se almacenarían durante dos años.

### ***Cambios en marcha***

Cuando Gareth sale de la urbanización con su coche, las verjas de hierro forjado se abren automáticamente y la cámara registra la hora exacta de la salida así como el número de ocupantes y las identidades del conductor y los pasajeros. En las carreteras, el reconocimiento automático de las matrículas lleva operativo en todo el país desde 2008 y ahora hay tantas cámaras que ya no vale la pena tratar de averiguar dónde se encuentran usando escáneres o mapas. En cualquier caso, el ordenador de mano que Gareth acopla en su coche está conectado con el sistema Galileo de navegación global por satélite así como a las cámaras gubernamentales con información de tráfico con lo que le ayuda a encontrar la ruta más rápida. El usar la ruta más corta además resulta más barato puesto que mediante el sistema ANPR el kilometraje de vehículo se carga automáticamente a su cuenta bancaria<sup>46</sup>.

### ***Biometría***

Casi todos los nuevos sistemas de identidad también usan algún tipo de dato “biométrico” o trazos corporales: las huellas dactilares, el escaneado del iris, la topografía facial y el escaneado de las manos se usan en diferentes pasaportes y sistemas de carné de identidad. Con frecuencia se nos presentan los datos biométricos como métodos infalibles. La idea es que la precisión se incrementará y se reducirá el fraude. Es posible olvidar o perder números PIN o contraseñas, pero el cuerpo humano proporciona un vínculo constante y directo entre un registro y la persona. Desde el 11-S, éstos se han fomentado especialmente en los EE.UU., y este país ejerce presión para la adopción de estándares comunes en los pasaportes biométricos.

Los sistemas de acceso biométricos (mediante el uso de voz y el escaneado de la mano, en particular) ahora son habituales para entrar en numerosos edificios de oficinas o propiedades de empresas privadas así como en algunos aeropuertos como, por ejemplo, el sistema Privium para el escaneado del iris en el aeropuerto de Schiphol en los Países Bajos, pero los sistemas biométricos también están saliendo a las calles. En las ciudades británicas también se han realizado experimentos con aplicaciones de software para la “identificación del rostro” automática en Newham (Londres), Birmingham, Tameside, Manchester y otros lugares. La identificación del rostro y otros sistemas de circuito cerrado de televisión biométricos todavía no funcionan correctamente en exteriores o en calles atestadas de gente que camina rápidamente. No obstante, se está realizando una inversión considerable para su mejora.

### ***¡Su salud es nuestro negocio!***

En 2016, Gareth trabaja como jefe de un centro de llamadas. Al igual que en 2006, se realiza un seguimiento de los empleados cada minuto del día mediante un ordenador que registra todas las actividades que realizan y cuánto tiempo dedican a las mismas. No obstante, la vigilancia en las contrataciones y en el otorgamiento de prestaciones se ha intensificado. Los empleados ahora tienen que someterse a una serie de pruebas biométricas y sicométricas así como cuestionarios sobre su estilo de vida. Gareth cree que es importante que el perfil del estilo de vida del empleado concuerde con los de los clientes para asegurar una mejor atención al cliente<sup>47</sup>. También le preocupa que los empleados no participen en deportes de riesgo, como el rugby o el ciclismo de montaña, puesto que esto puede causar largos periodos de ausencia debido a lesiones. Las pruebas biométricas, que suponen la toma de muestras de saliva y de orina, son analizadas fácilmente por la enfermera de que disponen en las instalaciones mediante un kit barato, lo cual significa que el empresario puede evaluar si el empleado potencial supone algún riesgo para la productividad como consecuencia de problemas de salud o adicción a algún tipo de droga. Esto también permite a la organización diseñar un paquete flexible de beneficios dependiendo del estado de salud del empleado. Algunos solicitantes de trabajo muy interesados han comenzado a facilitar voluntariamente información sanitaria y ahora con frecuencia la empresa descarta los currículos que no contienen esta información. Debido a la preocupación sobre la salud de los empleados, muchas empresas han comenzado a tomar iniciativas propias. En colaboración con los gimnasios locales, los empleados usan sus tareas de acceso inteligentes RFID para obtener descuentos. Sus visitas al gimnasio aparecen en su registro electrónico de empleo y con frecuencia se cuestiona a los empleados que no asisten regularmente sobre su estilo de vida en las revisiones salariales anuales. Las pruebas sicométricas periódicas también muestran a la gerencia si las actitudes de los empleados son compatibles con la cultura y los valores de la empresa.

#### *Localización, seguimiento y control electrónico*

La vigilancia consiste cada vez más en hacer un seguimiento de las personas, mediante GIS (Sistemas de Información Geográfica), GPS (Sistemas de Posicionamiento Global, chips RFID (identificación por radiofrecuencia), y tarjetas inteligentes de identificación, transpondedores o señales de radio emitidas por teléfonos móviles u ordenadores portátiles.

Tanto el GPS como la RFID se consideran cada vez más como soluciones para la aplicación de la ley y la gestión del personal. El seguimiento electrónico también se ha introducido como una condición para otorgar la libertad condicional y se colocaron dispositivos electrónicos de seguimiento a aproximadamente 631 adultos y 5.751 delincuentes juveniles, algunos de tan sólo doce años de edad, lo que les permitía vivir en sus domicilios a la espera de sus juicios, en vez de permanecer en prisión preventiva<sup>48</sup>. También se somete a los delincuentes que salen de prisión a un seguimiento electrónico, bien como condición de una puesta en libertad anticipada en virtud del Programa de Detención Domiciliaria (*Home Detention Curfew Scheme, HDC*<sup>49</sup>) o como una condición de su puesta en libertad condicional<sup>50</sup>.

Hasta hace poco el RFID se restringía a los grandes contenedores de transporte marítimo, bienes de consumo y diferentes tipos de tarjetas inteligentes. Recientemente, se ha producido un cambio considerable que ha pasado mayoritariamente desapercibido: la implantación en seres vivos. Los chips con información sobre registros de vacunas y propiedad han reemplazado gradualmente a los requisitos de cuarentena para las mascotas caseras en la UE desde el 28 de febrero de 2000 hasta el

programa PETS, que desde entonces se ha extendido más allá de las fronteras europeas<sup>51</sup>. La primera aplicación en seres humanos a los que se ha implantado chips RFID ha sido en los EE.UU. en personas de edad avanzada que sufren enfermedades degenerativas y aproximadamente 70 personas ya han recibido un implante que permite a sus cuidadores localizarlos fácilmente<sup>52</sup>. Los investigadores y entusiastas de la tecnología también se han aplicado autoimplantes desde hace años<sup>53</sup>, y al menos una cadena de discotecas en España ofrece a sus clientes la oportunidad de que sus chips implantados les permitan contener efectivo y privilegios de acceso<sup>54</sup>. No obstante, en febrero de 2006 se produjo un cambio de dirección cuando una empresa de seguridad en Ohio, EE.UU. implantó chips RFID a dos de sus trabajadores para permitirles el acceso a las propiedades de la empresa<sup>55</sup>. En la actualidad se está debatiendo seriamente en algunos sitios web de tecnología la posibilidad de que todo el mundo lleve un implante.

Mirando hacia el futuro, las empresas consideran tanto los dispositivos de RFID como el GPS simplemente como un medio para producir marketing personalizado en tiempo real para clientes particulares, mediante los que ofrecer descuentos en dispositivos móviles a tiendas minoristas en una ubicación determinada, por ejemplo. Los desarrollos constantes en la aplicación de datos de ubicación en tiempo real a los perfiles de los consumidores proporcionará otro nivel más de datos que ayudarán a la empresas a dirigir campañas de marketing a consumidores particulares y, potencialmente, también permitirán el seguimiento de los mismos por parte de los representantes de la ley y otros dispositivos de vigilancia gubernamentales.

### ***El nuevo “paisaje de marca”***

En 2016, cuando la familia Jones visita el centro comercial de su localidad, las cámaras de CCTV y los guardias de seguridad continúan estando presentes. Pero algunas cosas han cambiado. Además de controlar el nivel de criminalidad, la modelación espacial del “paisaje de la marca” (en inglés “brandscape”<sup>56</sup>) y los cambios publicitarios según el flujo de diferentes categorías de consumidores se han convertido ahora una estrategia prioritaria. Las cadenas minoristas permiten que el centro comercial acceda a una enorme base de datos compartida, modelada de acuerdo con los datos de las tarjetas de fidelidad, para generar información sobre los compradores. El sistema está basado en prendas con dispositivos electrónicos RFID, escáneres por todas partes y conjuntos de datos sobre los consumidores. Los escáneres a las puertas de las tiendas registran los identificadores únicos que se encuentran en los dispositivos RFID integrados en las prendas de ropa de los compradores. Carteles publicitarios inteligentes situados a la altura de los ojos anuncian una gama selecta de productos dirigidos a cada consumidor en tiempo real. Sara está encantada de ver aparecer en la pantalla la nueva descarga de su grupo favorito y Toby descubre información sobre modificaciones especiales para su mundo de juego en línea favorito. Los mensajes de marketing también se pueden enviar a los ordenadores de mano de los consumidores cuando pasan cerca de determinadas tiendas.

Ahora se invita a los clientes de alto valor a que se inscriban en un nuevo programa en el que no es necesario disponer de dinero en efectivo. Esto permite a los clientes más “valorados”<sup>57</sup> sustituirlo mediante la implantación de un chip<sup>58</sup>. El coste del implante es de 200 libras esterlinas pero con todos los descuentos especiales en las tiendas<sup>59</sup> pronto se amortiza (y mucho más). Las personas pueden cargar el chip con dinero y pagar en las diferentes tiendas escaneando su brazo, en lugar de usar tarjetas de crédito, de débito o las de las propias tiendas. Los compradores con el chip implantado además obtienen acceso a una sala VIP, spa y centro de masaje en las instalaciones comerciales. La estrategia de marketing de este sistema “sin dinero en efectivo” informa a los

consumidores de que dejarán de ser un objetivo importante para los ladrones y carteristas e incluso del fraude de tarjetas de crédito. Se han oído rumores acerca de clientes asaltados en el aparcamiento a los que les han cortado los chips del brazo, pero los operadores afirman que se trata de una “leyenda urbana”. Papá Gareth, que estaba considerando la posibilidad de suscribirse al sistema, ha visto un programa de televisión en el que se decía que los chips son atacados por virus informáticos y esto le preocupa especialmente porque las consecuencias de ser sospechoso de fraude ahora son mucho más serias. Como resultado de los algoritmos de predicción más sofisticados basados en los perfiles de consumo individual, el recibir una llamada del banco ahora equivale casi a ser declarado culpable: las tarjetas se desactivan automáticamente y el consumidor está obligado a presentar ante el banco pruebas independientes de quién es y dónde se encontraba.

## Flujos de datos

Los datos recopilados por las tecnologías de la vigilancia fluyen a través de las redes informáticas. Muchas personas pueden consentir a suministrar sus datos en un contexto determinado, pero ¿qué ocurre si esos datos se transfieren a otro contexto? Sin embargo, el público en general y las agencias que comparten datos tienen conocimientos muy limitados sobre adónde van exactamente a parar esos datos.

### *Desviación de uso*

La vigilancia parece seguir su propia lógica particular. Pero es necesario cuestionar, examinar y controlar esa lógica, en particular cuando los datos fluyen de un contexto a otro y la información recabada para una finalidad determinada acaba teniendo usos en un contexto nuevo y para fines distintos. Un ejemplo son las tarjetas de transporte Oyster en Londres, en las que los datos personales sobre el uso del transporte público son solicitados cada vez más en investigaciones policiales<sup>60</sup>. En la actualidad, los servicios de seguridad e inteligencia no sólo usan en la creación de perfiles de terroristas potenciales las mismas técnicas para la obtención de información desarrolladas para crear perfiles de consumidores, sino que a menudo esos mismos datos a partir de los que se crean los perfiles son exactamente los mismos. Se está permitiendo gradualmente que las tecnologías para el diagnóstico médico se deslicen sigilosamente hacia contextos más y más amplios, debilitando sus cualidades predictivas para la realización de diagnósticos positivos durante el propio proceso: es posible que aquellos que han recibido un diagnóstico equivocado se encuentren en una posición de desventaja. En el puesto de trabajo, las tecnologías para el seguimiento de los empleados en ocasiones pueden aportar más información de la requerida y la directiva siente la tentación de ampliar sus prácticas de seguimiento sin consultar con sus empleados lo que puede influir en su salario o en decisiones sobre ascensos.

### *Convergencia*

Cada vez más sistemas se diseñan con estos flujos de datos en mente. La interoperabilidad es inherente y existe una creciente convergencia de tecnologías de vigilancia. Esto significa que pueden surgir productos nuevos de forma totalmente imprevista y desordenada. Por ejemplo, en la actualidad existe una gran presión para encontrar carnés de identidad que resulten efectivos para diversas finalidades: cruce de fronteras, control de fraude, acceso a información gubernamental y tal vez comercial (alquiler de vídeos) así como también semicomercial (bibliotecas). Esto otorga un poder inmenso a los archivos cuya información es esencial en las oportunidades vitales de cada persona a aquellos que controlan las bases de datos de identidad.

### *Hacia una vigilancia omnipresente*

Las tecnologías se encuentran en su punto álgido cuando se convierten en omnipresentes, se dan por sentadas y resultan mayoritariamente invisibles. Cada vez más, nos enfrentamos a diversos “puntos de tránsito” que debemos atravesar durante nuestra vida cotidiana, que implican *tanto* aspectos electrónicos como físicos estrechamente relacionados: una combinación de circuitos cerrados de televisión, datos biométricos, bases de datos y tecnologías de seguimiento. La vigilancia está cada vez más presente en todas partes y a todas horas: es omnipresente.

### **Clasificación social**

En la sociedad de la vigilancia, la “clasificación social” es endémica. En los ámbitos del gobierno y el comercio se analizan y clasifican grandes bases de datos de información personal para definir los mercados objetivo y las poblaciones de riesgo<sup>61</sup>. Una vez que se pasa a formar parte de una categoría, resulta difícil escapar de esa etiqueta. Desde los sucesos del 11-S, es posible que este proceso de clasificación haya contribuido a una mayor seguridad en el transporte aéreo (ello nunca se sabrá con certeza), pero estamos seguros de que uno de sus efectos ha sido la creación de perfiles rudimentarios de grupos, especialmente musulmanes, que ha tenido como consecuencia molestias, dificultades e incluso torturas.

La clasificación social define cada vez más a la sociedad de la vigilancia. También hace que diferentes grupos tengan diferentes oportunidades y con frecuencia se traduce en formas sutiles y a veces no previstas de clasificar a las sociedades, formulando políticas sin un debate democrático previo. Los sistemas invisibles que se dan por sentados para la descongestión del tráfico y el transporte público inteligente tienen sus usos, pero ambos dividen a la ciudad en dos grupos, uno que puede viajar de forma relativamente libre y otro al que viajar le resulta difícil. Al mismo tiempo, se pueden usar para el control de los niveles de delincuencia y para la seguridad nacional. Nadie ha votado directamente la instauración de tales sistemas, sino que han llegado como resultado de un impulso para lograr una mayor eficacia y efectividad en los servicios públicos, de la presión por parte de las grandes empresas tecnológicas, el incremento en el “riesgo” como tema clave en la sociedad y la idea de que deberíamos aplicar el menor esfuerzo posible en la prevención de peligros.

### **Sin perder de vista a los niños**

En 2016, el control por medios electrónicos y el seguimiento se han convertido en una parte absolutamente fundamental de la educación<sup>62</sup>. Como resultado de una serie de casos de gran repercusión pública en los que algunos estudiantes se perdieron, resultaron heridos o murieron, numerosos colegios, en particular escuelas de primaria e incluso guarderías, comenzaron a preocuparse por no perder de vista a sus pupilos para evitar ser demandados<sup>63</sup>. Las escuelas primarias comenzaron a adoptar pruebas para detectar el consumo de drogas, en respuesta a la política gubernamental destinada a identificar niños problemáticos a una edad temprana, reducir el absentismo escolar y mejorar la concentración en el aula (muy importante en vista de las siempre presentes listas de clasificación)<sup>64</sup>. En el centro escolar Toby Jones, se introdujo un sistema de tarjetas que la mayoría de las familias usaban para controlar lo que sus hijos comen. Al cabo de tres años, el supermercado NSC compró esa empresa de tarjetas al considerarla como un camino de entrada en los lucrativos mercados juveniles y lograron obtener un reconocimiento de su marca mediante la aportación de material escolar. Se pidió a los padres que pasasen la tarjeta de sus hijos en la caja del supermercado, de modo que se identificaba a la escuela, al alumno y a los padres, y NSC proporcionaría material escolar extra según el gasto que los padres hiciesen en sus compras. Algunos de los proveedores<sup>65</sup> clave de NSC comenzaron a instalar sus máquinas expendedoras en las escuelas. El colegio Toby continuó participando en el programa y cada vez que llegaba material nuevo a la escuela se podía ver fácilmente la marca NSC en un lugar destacado. La autoridad educativa local realizaba un seguimiento de los tipos de alimentos que se consumían en la escuela Toby y usaba los datos para informar de diversas campañas sobre “alimentación sana” que emprendían. Poco a poco la tarjeta se fue integrando cada vez más hasta el punto de contener información no sólo sobre los alimentos que los alumnos compraban para las comidas, sino también sobre su nivel de asistencia, datos sobre sus logros escolares, actividades extraescolares, resultados de pruebas sobre consumo de drogas y acceso a Internet, e incluso se usaban como parte de la clase de ciudadanía de los estudiantes. Mientras que el incremento de la vigilancia en los colegios aportó unos beneficios considerables tanto a las escuelas como a los propios alumnos, los niños comenzaron a aceptar una vigilancia cada vez más intrusiva, el control de sus movimientos y el seguimiento remoto de lo que comían y adónde iban, como si se tratase de algo normal...

### **Dependencia tecnológica**

Es posible que se produzcan algunas respuestas tecnológicas a la vigilancia: algunas de las llamadas tecnologías para la mejora de la privacidad (en inglés, *privacy-enhancing technologies*, PET) podrían ayudar a frenar el crecimiento de la vigilancia tecnológica y se debería fomentar su uso cuando sea apropiado. No obstante, ni el mal funcionamiento de las mismas ni las PET deben significar que la respuesta es simplemente “mejores tecnologías”. Cuanto mayor sea la dependencia por parte de estados, organizaciones, individuos y sociedad en general de la tecnología de la vigilancia, más se producirá una “dependencia” que evitará la consideración de otras opciones para lograr los mismos objetivos así como un vacío de conocimiento que incrementará nuestra dependencia en competencias fuera del sistema democrático. Por ejemplo, con la introducción de los carnés de identidad, la dependencia de los mismos por parte del gobierno para que proporcionen tanto conocimientos tecnológicos como comerciales se incrementará inevitablemente.

Debemos ser precavidos cuando se nos ofrece arreglar problemas técnicos con soluciones técnicas. Como veremos más adelante, el verdadero mundo de la sociedad de la vigilancia es demasiado complejo para respuestas tan superficiales. También debemos preguntarnos si el gobierno dispone de las herramientas necesarias para realizar una regulación significativa de las cada vez más complejas tecnologías y prácticas de la vigilancia. ¿Es posible volver a meter al genio en la lámpara?

## Fallos tecnológicos

Por supuesto, las promesas hechas por las diferentes tecnologías casi nunca se cumplen tal como está previsto. La tecnología biométrica para el programa USVISIT, por ejemplo, se redujo de los escaneados del iris previstos a la toma de muestras de huellas digitales, por motivos logísticos<sup>66</sup>. Del mismo modo, los elementos biométricos del programa e-Borders (fronteras electrónicas) del Reino Unido se han visto sujetos a problemas de implementación<sup>67</sup>. El reconocimiento facial continúa sin dar resultados óptimos en situaciones de la vida real. La Oficina de registros criminales (Criminal Records Bureau) reveló que se han atribuido erróneamente antecedentes penales a aproximadamente 2.700 personas y como resultado de estos dobles de información incorrecta, a algunos de ellos se les negaron ofertas de empleo<sup>68</sup>. En el sistema de identidad propuesto en el Reino Unido se calcula que es probable que una de cada seis personas no pueda usar su carné de identidad debido a problemas técnicos para introducirlos en el sistema<sup>69</sup>.

Es posible que tales errores limiten el acceso a lugares o servicios, pero en otros casos, por ejemplo en la vigilancia médica, podrían poner vidas en peligro ya que son mucho más habituales de lo que la mayoría de la gente piensa. Los fallos o la deficiencia tecnológicos, por lo tanto, pueden acabar teniendo resultados mucho más negativos en las opciones de supervivencia que un sistema que funcione correctamente.

## ¿Qué consecuencias tiene la sociedad de la vigilancia?

Aunque la sociedad de la vigilancia nos proporciona beneficios y derechos, también aporta consecuencias negativas, algunas de las cuales son muy crudas y potencialmente irreversibles. Cualquier debate público acerca de la vigilancia debe tomar en consideración sus efectos sobre la privacidad, los valores éticos y los derechos humanos; su impacto sobre la inclusión y exclusión social; cambios en los niveles de elección, de poder y de concesión de derechos; si se podrá responsabilizar a los encargados de gestionar tales sistemas y si los procesos de vigilancia son transparentes o no.

### *Privacidad, ética y derechos humanos*

Muchos de los argumentos actuales acerca de la vigilancia están basados en ideas sobre la “privacidad”. Desde la década de 1970 se han promulgado numerosas leyes de protección de datos en Europa y leyes de privacidad en otras partes del mundo. No obstante, ha resultado difícil persuadir a los responsables de formular políticas de cualquier otra dimensión *social* más profunda de la privacidad<sup>70</sup>, y menos aún de la necesidad de enfrentarse a problemas asociados con la sociedad de la vigilancia como tal. En muchos casos, las personas ni siquiera saben que algo va mal y aún menos disponen de la capacidad para identificar qué es, adónde dirigir su queja y cómo obtener un resarcimiento.

La privacidad es vital, pero la sociedad de la vigilancia plantea dilemas sobre derechos éticos y humanos que van aún más allá. No se debería pretender simplemente que las personas normales y corrientes tengan que protegerse a sí mismas. A continuación se exponen los tres temas claves en este ámbito:

### *Exclusión social y discriminación*

Tal como se muestra en el Informe completo, la vigilancia varía en intensidad, tanto geográficamente como en relación con la clase social, el origen étnico y el género de las personas. La vigilancia, la invasión de la privacidad y la protección de la misma crean diferencias entre los grupos sociales, favoreciendo a algunos y perjudicando a otros. La vigilancia ha crecido paralelamente a los cambios en la salud y el bienestar y, en muchos casos, estos servicios estatales se han visto reducidos a una simple gestión de riesgos, que requiere un conocimiento pleno de la

situación. Por ello, se busca la obtención de datos personales para determinar adónde dirigir los recursos<sup>71</sup>. Y, puesto que las redes de vigilancia permiten un alto grado de coordinación, las compañías de seguros pueden trabajar conjuntamente con la policía y los supermercados pueden combinar sus fuerzas con otros colectores de datos con muchísima más facilidad. El resultado es que con frecuencia las zonas conflictivas se encuentran predominantemente en sectores de etnia no blanca y los grandes supermercados suelen establecerse en barrios de clase alta o en las afueras de las ciudades, de forma que resultan más accesibles a aquellos que poseen coche.

### ***¿Soluciones sociales totales?***

En 2016, las zonas residenciales están más claramente divididas entre comunidades en recintos privados, como donde vive la familia Jones, patrulladas y controladas por grandes empresas de seguridad altamente equipadas, y antiguos barrios con viviendas de protección oficial y de bajo coste como la barriada Dobcroft. Para los Jones, los sistemas de cámaras y de identificación en la comunidad y entorno a ella reducen los costes del seguro al mínimo<sup>72</sup>. En la barriada Dobcroft, el trabajo que realiza Yasmin en un equipo de labores sociales multiagencia ha sido subcontratado a un consorcio privado llamado, de modo optimista, Soluciones Sociales Totales. SST cobra por realizar el seguimiento y hacer respetar el cumplimiento de los “Programas de Comportamiento Personal”<sup>73</sup> del que todos los habitantes de la barriada Dobcroft son “clientes” desde su nacimiento<sup>74</sup> (y algunos de ellos son identificados incluso antes<sup>75</sup>). Muchos de los que se encuentran en niveles altos de PCP, como la libertad condicional<sup>76</sup>, ahora llevan chips RFID activos implantados que se comunican automáticamente con los sensores instalados en sus casas y en las entradas de la barriada<sup>77</sup>. En teoría estos implantes son voluntarios, pero al igual que los programas de las tiendas y de las escuelas, el cumplimiento del mismo otorga ciertas ventajas, una de las cuales y no menos importante es la puesta en libertad de la prisión preventiva. En la actualidad la barriada Dobcroft también está sujeta a uno de sus “toques de queda generales” periódicos tras la supuesta identificación por parte de una anciana del pueblo residencial para jubilados Vistalegre de algunos “jóvenes” de la barriada como los causantes de disturbios. La mujer descubrió las actividades sospechosas en las cámaras de vídeo de vigilancia local, que se pueden ver en los canales de seguridad locales de la televisión digital, la cual incluye asimismo un “registro de delincuentes” de todos aquellos que han incumplido sus PCP<sup>78</sup>. Está prohibido a todos los menores de 18 años entrar o salir de la barriada entre las 6 de la tarde y las 6 de la mañana.

### *Elección, poder y concesión de derechos*

Entonces, ¿tenemos voz y voto para enfrentarnos a la sociedad de la vigilancia? La gente corriente puede ejercer una influencia importante cuando insiste en el cumplimiento de las normas y leyes, cuestionan el sistema o se niegan a que sus datos sean utilizados para fines sobre los que carecen de la suficiente información o sobre los que albergan dudas.

Con todo, ¿hasta qué punto pueden los individuos y los grupos elegir su exposición a la vigilancia y limitar la recogida y uso de información personal? Con frecuencia, los sistemas de vigilancia son demasiado técnicos para que los entiendan personas inexpertas y se ocultan en las estructuras cotidianas y en los sistemas de la sociedad: en el trabajo, en el tiempo libre, en el hogar, en las escuelas, en los viajes y las comunicaciones y en los servicios públicos. Parece más difícil poder cambiar la situación. Por ejemplo, hasta que no se produce algún escándalo relacionado con el robo de identidad, los consumidores no se percatan de la elaboración de perfiles personales que llevan a cabo las grandes empresas<sup>79</sup>. Aun así, se suele prestar atención sobre todo a los aspectos de seguridad (cómo impedir otros fraudes similares), más que a cómo poner freno a la capacidad de las empresas y de las agencias estatales sobre los datos. Los individuos se encuentran en una seria desventaja a la hora de controlar el impacto de la vigilancia.

### *Transparencia y responsabilidad*

Las infraestructuras de las empresas, de transporte y gubernamentales disponen de capacidades de vigilancia que se multiplican, mientras que a los individuos y grupos les resulta difícil descubrir cómo se utiliza su información personal, quién la administra y con qué fines. Sin embargo, poco a

poco sus datos personales se utilizan para dar forma a las oportunidades que se les presentan en sus vidas y guiar las elecciones que realizan. Las organizaciones deberían asumir su responsabilidad, especialmente cuando se produce una vigilancia de gran intensidad de forma rutinaria con consecuencias potencialmente nocivas. Debemos pasar de la autoprotección de la privacidad a la responsabilidad de los manipuladores de datos, además del trabajo de los reguladores oficiales para velar por el cumplimiento de los controles y ejercer presiones para reducir al mínimo la vigilancia.

## El desafío normativo

¿Es posible reglamentar la vigilancia para mantener sus efectos negativos bajo control y hacerla compatible con el tipo de sociedad y democracia que deseamos lograr<sup>80</sup>? El exigir la realización de evaluaciones acerca del impacto de nuevos proyectos sobre la privacidad y la vigilancia contribuiría a la concienciación pública y al debate, y añadiría una dimensión importante a los sistemas reglamentarios. Existen muchas leyes y códigos de conducta para la protección de la privacidad. También existen tecnologías que proporcionan cierta protección. Existen agencias reguladoras dedicadas que aplican la ley, ayudan con las quejas de la gente y tratan de influir sobre las políticas gubernamentales y los avances empresariales. Existen los grupos de presión y los medios de comunicación que nos alertan de los peligros de la vigilancia. Pero el poder y la eficacia de esos mecanismos reglamentarios es cuestionable; necesitan ser reconsiderados y mejorados. En cualquier caso, mientras que la protección de la privacidad es parte de la historia, no supone la historia completa. Mayor número de personas deben comprender el significado de la vigilancia y participar en decidir qué se debe hacer al respecto, si ha de hacerse algo, para que esté al servicio de las personas de forma apropiada. Pero no es suficiente con que su reglamentación se realice únicamente en un país o incluso en un grupo de países como la Unión Europea. Los flujos de información que forman parte de la vigilancia son ciertamente globales; como también lo son los movimientos y actividades que se mantienen bajo vigilancia. Existe la necesidad de una reglamentación más integrada y más global para enfrentarse a esos desafíos.

### ***La sala de los espejos***

Aunque la vigilancia está en todas partes en 2016, las personas, especialmente aquellas con un cierto nivel educativo o suficientemente adinerados para apreciarla o poder permitírsela, son cada vez más conscientes de ella y logran encontrar nuevas maneras de convivir con ella. Gareth Jones se ha suscrito a un servicio de gestión de la información personal que controla su "sombra de datos" en línea, corrige automáticamente información incorrecta contenida en las bases de datos públicas y en algunas de consumidores y le alerta de cualquier otro problema. Su costoso ordenador de mano también le permite bloquear mensajes publicitarios de los anunciantes. Pero, lamentablemente, no todo el mundo tiene la capacidad para acceder y modificar del mismo modo su información personal. Aquellos menos capacitados en la gestión de la información personal o con menores posibilidades para pagar a otros para que gestionen su información en su nombre se encuentran en seria desventaja. Los defensores de un acceso y cambio más fácil de la información personal en poder del estado y de las empresas privadas colaboradoras de éste han logrado que así sea, pero el acceso es uno de los numerosos factores que ahora están supeditados a poseer un carné de identidad. Esto ha dado lugar a un pulso cada vez más incómodo, y hasta ahora no resuelto, entre los ciudadanos y el estado sobre quién sabe qué, quién tiene la propiedad de los datos y quién tiene derecho a cambiarlos. Pero en 2016, la gente está más acostumbrada a observar que a ser observada. Muchos se ofrecen como voluntarios para que toda su vida sea vigilada o para el registro de sus actividades vitales (*life logging*), anotando casi todo lo que hacen para archivarlo o ponerlo directamente en línea<sup>81</sup> en tiempo real. Existe una gran cantidad de vigilancia del vigilante por parte de defensores radicales que consideran que el estado "no hace lo suficiente" para controlar el terrorismo, la delincuencia y la inmigración ilegal<sup>82</sup> con lo que han proliferado sitios web no oficiales de los "sospechosos", lo que ha llevado a todo tipo de errores e identificaciones equivocadas<sup>83</sup>. Inconformistas, artistas y surrealistas, todos juegan y resisten la vigilancia omnipresente por todo tipo de medios, incluida la inutilización de dispositivos de vigilancia públicos<sup>84</sup>, el uso de tecnologías de "contravigilancia" que reflejan o contraatacan la vigilancia<sup>85</sup>. A algunos activistas anticapitalistas, como a Aaron y a Ben, les gusta pasar las tardes de los sábados pegando láminas de aluminio

altamente adhesivas y pequeños transmisores de microondas a pilas en las entradas de las tiendas para interferir las señales inalámbricas<sup>86</sup>. El registro de las actividades vitales no es tan maravilloso como podría parecer y con aplicaciones de software cada vez más sofisticadas para la gestión de datos y producción de vídeos, vidas enteras se pueden ajustar o incluso crear de cero con fines que van desde el puro pasatiempo pasando por la subversión hasta el fraude. En 2016 cada vez existe un mayor número de sombras de datos totalmente virtuales, que no tienen un homólogo en la vida real, pero que parecen existir y son sujetos de la gestión de la información y la vigilancia en línea por parte de sistemas automatizados que trabajan silenciosa e invisiblemente, habitantes de una sala de espejos interminable...

## Referencias

Nota: todas las páginas web estaban accesibles el 1 de septiembre de 2006.

<sup>1</sup> Estas visiones fugaces de un posible futuro están tomadas de la Sección C del Informe completo, que también incluye “Una semana en la vida” de una familia típica en 2006.

<sup>2</sup> Hace varios años que el ejército de los EE.UU. usa los UAV: en la actualidad el ejemplo más conocido es la aeronave teledirigida de reconocimiento “Predator” usada en Irak; véase: “Predator RQ-1 / MQ-1 / MQ-9 Unmanned Aerial Vehicle (UAV), USA”, *airforce-technology.com*, 2006, <http://www.airforce-technology.com/projects/predator/>. En el Reino Unido se han sugerido diversos usos, véase: Jha, A., “On the horizon... pilotless planes as fishermen's and firefighters' friends”, *The Guardian*, 30 de agosto de 2006, <http://www.guardian.co.uk/science/story/0,,1860825,00.html>. La policía de Los Angeles ya está experimentando con pequeños aviones espía teledirigidos llamados “SkySeer”: Bowes, P., “High hopes for drone in LA skies”, *BBC News*, 6 de junio de 2006, <http://news.bbc.co.uk/1/hi/world/americas/5051142.stm>.

<sup>3</sup> A lo largo de la historia se han usado eventos deportivos importantes para probar e introducir nuevas tecnologías de vigilancia. Por ejemplo, sobre las cámaras de CCTV y el Mundial de Japón 2002, véase: Abe, K., (2004) “Everyday policing in Japan: surveillance, media, government and public opinion”, *International Sociology*, 19, 215–231; y sobre cámaras de CCTV y las Olimpiadas de Atenas, véase: Samatas, M. (2004) *Surveillance in Greece*, Athens: Pella.

<sup>4</sup> Véanse los informes periciales Crime and Justice and Infrastructure Expert Reports. Uno de los problemas fundamentales del reconocimiento facial ha sido el ángulo de visión de las cámaras de CCTV; véase, por ejemplo: Introna, L. y Wood, D. (2004) “Picturing algorithmic surveillance: the politics of facial recognition systems”, *Surveillance & Society*, 2(2/3): 177-198.

<sup>5</sup> El control del orden en las ciudades ya se está entregando a sociedades público-privadas, organizaciones para la gestión de los centros urbanos (<http://www.atcm.org/>) y BID. Según el gobierno, los BID proporcionan “inversión en el entorno comercial local mediante la provisión de servicios de valor añadido”: <http://www.ukbids.org/>. En 2016 una de los aspectos regulatorios más importantes es la transferencia de información entre el estado y las empresas de seguridad privadas que actúan en nombre del estado o en su lugar, especialmente ahora que el Ordenador Nacional de la Policía (PNC) engloba tantas bases de datos y que el cuerpo de policía y los servicios de libertad condicional, penitenciarios y sociales están tan entrelazados.

<sup>6</sup> Muchos cuerpos de policía ya los están probando, véase por ejemplo: “Pocket computers put police ‘in the picture’”, *West Yorkshire Police*, 28 de marzo de 2006, <http://www.westyorkshire.police.uk/section-item.asp?sid=12&iid=2226>; y el programa “Airwave” (véase el informe pericial Crime and Justice Expert Report) está diseñado para integrarlos al mismo.

<sup>7</sup> De nuevo, en muchas zonas ya se están introduciendo cámaras integradas en los cascos conectadas en directo con las salas de control; véase por ejemplo: “Police use anti-yob head cameras”, *BBC News*, 23 de marzo de 2006, [http://news.bbc.co.uk/1/hi/wales/north\\_east/4836598.stm](http://news.bbc.co.uk/1/hi/wales/north_east/4836598.stm).

<sup>8</sup> En 2016, la policía y sus aliados privados tienen acceso a prácticamente todas las bases de datos ahora conectadas mediante el PNC.

<sup>9</sup> En 2016, todavía se continúan manteniendo debates en los medios de comunicación así como entre los políticos sobre el derecho de la policía a hacer esto, pero se argumenta que los carnés de identidad proporcionan una manera fácil de determinar las buenas intenciones de una persona y no se puede asumir el riesgo de suponer la inocencia de aquellos individuos que no lo tienen.

<sup>10</sup> Ford, R., “Beware rise of Big Brother state, warns data watchdog”, *The Times*, 16 de agosto de 2004, [http://www.timesonline.co.uk/article/0,,2-1218615\\_1,00.html](http://www.timesonline.co.uk/article/0,,2-1218615_1,00.html).

<sup>11</sup> El grado de extensión completo de la vigilancia en la vida cotidiana de las personas se encuentra documentado en la Parte C del Informe completo.

<sup>12</sup> Datos obtenidos de *SecurityStockWatch.com 100 Index*, agosto de 2006: <http://www.securitystockwatch.com/>.

<sup>13</sup> Véase, por ejemplo; “The future of screening”, *BBC News*, 14 de diciembre de 2002, <http://news.bbc.co.uk/1/hi/health/2570787.stm>.

<sup>14</sup> McKie, R., “Icelandic DNA project hit by privacy storm”, *The Observer*, 16 de mayo de 2004, <http://observer.guardian.co.uk/international/story/0,6903,1217842,00.html>. Rose, H. (2001) *The Commodification of Bioinformation: The Icelandic Health Sector Database*, Londres: The Wellcome Trust.

<sup>15</sup> Esta cuestión se estudia en Lyon, D. *Surveillance after September 11*, Cambridge, Reino Unido: Polity Press, págs. 45–48, 142 y sig.

<sup>16</sup> Garton Ash, T. (1997) *The File: A Personal History*, Nueva York: Vintage.

<sup>17</sup> Las transacciones en efectivo, por ejemplo, aunque por lo general no se pueden relacionar directamente con un consumidor específico, con frecuencia son analizadas comparándolas con transacciones anteriores similares y tipos de consumidores que han realizado las mismas de compras.

<sup>18</sup> Véase Fink, J. y Kosba, A. (2000) “A review and analysis of commercial user modeling servers for personalization on the world wide web”, *User Modeling and User-Adapted Interaction*, 10, 209–249.

<sup>19</sup> The Wanless Report (2002) *Securing Our Future Health: Taking a Long-Term View: Final Report*, Londres: HM Treasury.

<sup>20</sup> PITO (2005) *Police Information Technology Organisation, Annual Report 2004 – 2005*, HC 261, Londres: The Stationery Office.

<sup>21</sup> Randerson, J., “DNA of 37% of black men held by police”, *The Guardian*, 5 de enero de 2006, <http://www.guardian.co.uk/frontpage/story/0,,1678168,00.html>.

<sup>22</sup> PITO (2006) *Facial Images National Database (FIND)*, <http://www.pito.org.uk/products/FIND.php>.

<sup>23</sup> ACPO (Association of Chief Police Officers) (2002) *Infinet: A National Strategy for Mobile Information*, Association of Chief Police Officers.

<sup>24</sup> La creación de perfiles informales sin lugar a duda ya sucede y viene sucediendo desde hace mucho tiempo. La policía del Reino Unido también la ha propuesto como una política oficial, véase: “No racial profiling by anti-terror police, says minister” *Times Online*, 2 de agosto de 2005, <http://www.timesonline.co.uk/article/0,,22989-1717624,00.html>. Para información de apoyo, véase: “Racial Profiling: Old and New”, *ACLU*, <http://www.aclu.org/racialjustice/racialprofiling/index.html>.

<sup>25</sup> Véase el informe pericial Borders Expert Report.

<sup>26</sup> En 2004, la Autoridad de aviación civil internacional acordó unos principios para los Documentos de viaje legibles mecánicamente (MRTD). Este proceso ha sido promovido por la Iniciativa para la seguridad y facilitación de desplazamientos internacionales (SAFTI) del G8 actual: “G8 meeting at Sea Island in Georgia, USA - sets new security objectives for travel”, *Statewatch*, 2004, <http://www.statewatch.org/news/2004/jun/09g8-bio-docs.htm>.

Esto se produce pese a la preocupación sobre la facilidad para clonar los chips RFID: Johnson, B., “Hackers crack new biometric passports”, *The Guardian*, 7 de agosto de 2006, <http://politics.guardian.co.uk/homeaffairs/story/0,,1838754,00.html>. Ya se ha tomado nota del hecho de que los carnés de identidad del Reino Unido podrían transformarse o fusionarse con los pasaportes biométricos: Lettice, J., “UK biometric ID card morphs into £30 ‘passport lite’”, *The Register*, 8 de Julio de 2005, [http://www.theregister.co.uk/2005/07/08/id\\_card\\_as\\_passport/](http://www.theregister.co.uk/2005/07/08/id_card_as_passport/).

<sup>27</sup> Véase el informe pericial Consumer Expert Report. En 2016 todavía existen asuntos pendientes entre los estados y las empresas de seguridad fronteriza subcontratadas acerca de la cuestiones relacionadas con la propiedad intelectual de los datos de los desplazamientos. El gobierno británico sostiene su “derecho” a vender datos de identidad, tal como se propuso en 2006: Elliot, F., “ID plans: powers set to widen”, *The Independent*, 6 de agosto de 2006, <http://news.independent.co.uk/uk/politics/article1216000.ece>. La única voz que todavía continúa perdida es la de los ciudadanos.

<sup>28</sup> Los escáneres de cuerpo completo se fabrican en formas diversas y ya se están poniendo a prueba, por ejemplo, el Secure 1000 basado en rayos X de bajo nivel de Rapiscan:

<http://www.rapiscansystems.com/sec1000.html>, probado en el aeropuerto de Heathrow, véase: Lettice, J. “‘See through clothes’ scanner gets outing at Heathrow”, *The Register*, 8 de noviembre de 2004,

[http://www.theregister.co.uk/2004/11/08/heathrow\\_scanner\\_pilot/](http://www.theregister.co.uk/2004/11/08/heathrow_scanner_pilot/); y los escáneres de ondas milimétricas que QinetiQ está desarrollando y Eurotunnel está probando:

[http://www.qinetiq.com/home/newsroom/news\\_releases\\_homepage/2004/3rd\\_quarter/Next\\_generation\\_security\\_screening.html](http://www.qinetiq.com/home/newsroom/news_releases_homepage/2004/3rd_quarter/Next_generation_security_screening.html).

<sup>29</sup> Campbell, D. (1999) *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: the state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (AKA Interception Capabilities 2000)*, Luxemburgo: Parlamento Europeo, Dirección General de Investigación, Dirección A, El Programa STOA.

<sup>30</sup> En 2016, la mayoría de la gente ahora posee estos dispositivos que incorporan acceso inalámbrico a Internet y roaming, servicios de telefonía, navegación informática y más. La función de navegación también garantiza que se puede hacer un seguimiento de los dispositivos (y, por lo tanto, sus operadores).

<sup>31</sup> Galileo es la alternativa civil europea al sistema militar GPS de los EE.UU. El primer satélite se lanzó en 2004 y algunos servicios ya estarán operativos en 2008, véase: “Galileo, European Satellite Navigation System” CEC Directorate General Energy and Transport, [http://ec.europa.eu/dgs/energy\\_transport/galileo/intro/future\\_en.htm](http://ec.europa.eu/dgs/energy_transport/galileo/intro/future_en.htm).

<sup>32</sup> La actual Regulation of Investigatory Powers Act (RIP, Ley regulatoria de los poderes investigativos) permite una retención de registros limitada, pero se presupone que en 2016 la policía y los servicios de seguridad querrán que las restantes "lagunas" queden selladas, muy probablemente en respuesta a algún escándalo que haya tenido gran repercusión pública relacionado con el terrorismo o la pederastia.

<sup>33</sup> "Cracking" hace referencia a "el acto de introducirse ilegalmente en un sistema informático, *The New Hacker's Dictionary*, [http://www.outpost9.com/reference/jargon/jargon\\_toc.html](http://www.outpost9.com/reference/jargon/jargon_toc.html).

<sup>34</sup> Los MMOG, según algunos cálculos, en la actualidad cuentan con aproximadamente 13 millones de suscriptores, siendo el mayor de todos *World Of Warcraft*, <http://www.worldofwarcraft.com/index.xml>, junto con la familia de juegos coreanos *Lineage I*, <http://www.lineage.com/>, y *II*, <http://www.lineage2.com/>. Otros mundos virtuales son más bien como analogías del mundo real e incluyen *Second Life*: <http://secondlife.com>. Cada vez se convierten en más inmersivos y sus economías se entrecruzan más y más con el mundo real, hasta el punto de que algunos elementos parte del juego se canjean por dinero "real" en sitios web de subastas como, por ejemplo, *ebay*, <http://www.ebay.com>. Véase *MMOGCHART.COM*, <http://www.mmogchart.com/> para obtener algunos análisis estadísticos.

<sup>35</sup> Ya se han dado algunos casos de "vigilancia virtual"; véase, por ejemplo: "Confessions of a Virtual Intelligence Analyst", *Terranova*, 15 de marzo de 2006, [http://terranova.blogs.com/terra\\_nova/2006/03/confessions\\_of\\_.html](http://terranova.blogs.com/terra_nova/2006/03/confessions_of_.html). Los analistas de marketing ya han identificado significativos mercados virtuales, lo que quiere decir que las empresas están empezando en enfocar sus miras hacia los mundos de los juegos, véase por ejemplo: Burns, E., "Marketing Opportunities Emerge in Online Gaming Venues, *ClickZ*, 1 de agosto de 2006, <http://www.clickz.com/showPage.html?page=3623035>, y ya se han lanzado los primeros "carteles publicitarios virtuales", véase: Shields, M., "Massive Unveils Toyota Ad Units Within Anarchy", *Mediaweek*, 19 de julio de 2006, [http://www.mediaweek.com/mw/news/interactive/article\\_display.jsp?vnu\\_content\\_id=1002876380](http://www.mediaweek.com/mw/news/interactive/article_display.jsp?vnu_content_id=1002876380).

<sup>36</sup> Esto se derivó de una serie de incidentes a lo largo de varios años en los que se produjeron transposiciones de incidentes de los juegos MMOG a delitos en el mundo real; véase, por ejemplo: "Chinese gamer sentenced to life", *BBC News*, 8 de junio de 2005, <http://news.bbc.co.uk/1/hi/technology/4072704.stm>.

<sup>37</sup> McCahill, M. y Norris, C. (2003), "Estimating the Extent, Sophistication and Legality of CCTV in London", en M. Gill (ed.) *CCTV*, Leicester: Perpetuity Press.

<sup>38</sup> Norris, C. y Armstrong, G. (1999) *The Maximum Surveillance Society: The Rise of Closed Circuit Television*, Oxford: Berg, 42.

<sup>39</sup> Norris, C. (2006) "Closed Circuit Television: a review of its development and its implications for privacy", documento creado para la reunión trimestral del *Department of Home Land Security Data Privacy and Integrity Advisory Committee*, 7 de junio, San Francisco, CA.

<sup>40</sup> Gill, M. y A. Spriggs (2005). *Assessing the Impact of CCTV*. Londres: Home Office Research, Development and Statistics Directorate, 43, 60–61.

<sup>41</sup> Wilkins, G. y Additcott, C. (1998) *Motoring Offences England and Wales 1996*, Home Office Statistical Bulletin, Londres: Home Office; Ransford, F., Perry, D. Murray, L. (2005) *Motoring Offences and Breath Test Statistics: England and Wales 2003*, Home Office Statistical Bulletin, Londres: Home Office.

<sup>42</sup> McCahill y Norris, 2003, *op cit*.

<sup>43</sup> PA Consulting (2004) *Denying Criminals the Use of the Road*, [http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR\\_10,000\\_Arrests.pdf?view=Binary](http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10,000_Arrests.pdf?view=Binary).

<sup>44</sup> *ibíd.*: 6.

<sup>45</sup> *ibíd.*: 18.

<sup>46</sup> Existen numerosos programas potenciales. Véase, por ejemplo: Independent Transport Commission (2006) *Paying to Drive*, [http://trg1.civil.soton.ac.uk/itc/p2d\\_main.pdf](http://trg1.civil.soton.ac.uk/itc/p2d_main.pdf).

<sup>47</sup> Una desventaja de ello es que una organización contrataría a un tipo de persona determinado y, en consecuencia, tendría una mano de obra menos diversa (véase el informe *Workplace Surveillance Expert Report*).

<sup>48</sup> NPS (2006a) - National Probation Service - *Electronic Monitoring*: 6.

<http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes>.

<sup>49</sup> El programa HDC permite a todas aquellas personas condenadas a un periodo de prisión de entre tres meses y cuatro años a ser puestos en libertad con una anticipación de entre dos semanas y cuatro meses y medio, mediante una detención domiciliaria nocturna forzosa e impuesta a través de un seguimiento electrónico. En 2004/5 se pusieron en libertad anticipada a 19.096 personas en virtud de este programa (NPS, *op. cit.*:6).

<sup>50</sup> NPS, *op cit*.

- <sup>51</sup> Para obtener más datos, véase el sitio web del Department of Environment, Food and Rural Affairs (DEFRA) PETS: <http://www.defra.gov.uk/animalh/quarantine/pets/index.htm>.
- <sup>52</sup> La empresa responsable es Verichip Corporation: <http://www.verichipcorp.com/>.
- <sup>53</sup> Amal Graafstra es uno de los entusiastas destacados y defensores de la autoimplantación de chips. Se pueden encontrar explicaciones, imágenes y vídeo para su descarga en su sitio web en <http://amal.net/rfid.html>.
- <sup>54</sup> Graham-Rowe, D., "Clubbers chose chip implants to jump queues", *New Scientist*, 21 de mayo de 2004, <http://www.newscientist.com/article.ns?id=dn5022>.
- <sup>55</sup> Waters, R., "US group implants electronic tags in workers", *Financial Times*, 12 de febrero de 2006, <http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html>.
- <sup>56</sup> El origen del término "brandscape" está definido por el UK Design Council como "El alcance en la experimentación y reacción hacia una marca. Un término que abarca a todos aquellos que tocan e interactúan con la marca incluidos los clientes, proveedores, trabajadores, competidores, revendedores, distribuidores, socios, etc.": [http://www.design-council.org.uk/webdav/harmonise?Page/@id=6046&Session/@id=D\\_rPJLjJbFNakH0E0GQvIo&Document%5B@id%3D5232%5D/Chapter/@id=7](http://www.design-council.org.uk/webdav/harmonise?Page/@id=6046&Session/@id=D_rPJLjJbFNakH0E0GQvIo&Document%5B@id%3D5232%5D/Chapter/@id=7).
- <sup>57</sup> Los clientes más valorados se establecen mediante una comprobación de crédito y referencia a su perfil de consumidor. El ser un cliente valorado significa que es probable que realice un gasto superior. Los implantes se convierten en un símbolo de clase.
- <sup>58</sup> Véase Baja Beach (nd.) "Zona VIP," <http://www.bajabeach.es/>.
- <sup>59</sup> Esto permitirá a la base de datos registrar más elecciones particulares de determinados individuos.
- <sup>60</sup> Véase "Oyster data use rises in crime clampdown", *The Guardian*, 13 de marzo de 2006, <http://politics.guardian.co.uk/foi/story/0,,1730771,00.html>.
- <sup>61</sup> Véase el estudio clásico de Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, CO: Westview, 1993.
- <sup>62</sup> Ya se encuentra en estado embrionario en los EE.UU. Véase, por ejemplo: Leff, L. "Students ordered to wear tracking tags", *Associated Press*, 9 de febrero de 2005, <http://www.msnbc.msn.com/id/6942751/>.
- <sup>63</sup> Véase, por ejemplo.: "Neglect ruling in girl pond death", *BBC News*, 23 de marzo de 2006, [http://news.bbc.co.uk/1/hi/england/coventry\\_warwickshire/4837614.stm](http://news.bbc.co.uk/1/hi/england/coventry_warwickshire/4837614.stm).
- <sup>64</sup> En el Reino Unido, las listas de clasificación catalogan las escuelas según los resultados obtenidos por los alumnos en los exámenes.
- <sup>65</sup> Por ejemplo, Nestlé, Unilever, Pepsico, etc.
- <sup>66</sup> United States Visitor and Immigrant Status Indicator Technology (Tecnología indicadora de estatus para los inmigrantes y visitantes a los EE.UU.) está en vigor en todos los puertos de entrada por tierra, aire y mar desde 2004.
- <sup>67</sup> Véase: Amoore, L. (2006) "Biometric Borders: Governing Mobilities in the War on Terror", *Political Geography* 25(2): 336-351.
- <sup>68</sup> "Criminal records mix-up uncovered", *BBC News*, 21 de mayo de 2006, <http://news.bbc.co.uk/1/hi/uk/5001624.stm>.
- <sup>69</sup> Véase: Grayling, A.C. (2005) *In Freedom's Name: The Case against Identity Cards*, Londres: Liberty.
- <sup>70</sup> Véase el excelente estudio de los aspectos sociales de la privacidad en: Regan, P. (1995) *Legislating Privacy*, Chapel Hill: University of North Carolina Press.
- <sup>71</sup> Véase: Ericson, R. y Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.
- <sup>72</sup> La Association of British Insurers (ABI, Asociación de aseguradoras británicas) lo ha solicitado en un importante informe sobre la vivienda: ABI(n.d.) *Securing the Nation: The Case for Safer Homes*, Londres: ABI, 12. <http://www.abi.org.uk/BookShop/ResearchReports/Securing%20the%20Nation%20July%202006.pdf>.
- <sup>73</sup> Aquí se presupone que las órdenes contra comportamientos antisociales (Anti-Social Behaviour Orders, ASBO), los programas de supervisión intensivos y otros similares (véase el informe pericial Crime and Justice Expert Report) se han conglomerado en Programas de Comportamiento Personal para aquellos que encajan en determinados patrones de riesgo de infringir la ley. Puesto que todos los residentes de la barriada Dobcroft encajan con al menos un criterio por el mero hecho de vivir en un barrio donde es probable que se cometa algún delito, todos están sujetos a los PCP.
- <sup>74</sup> El creciente entusiasmo por las intervenciones prematuras ya se ha extendido a estas edades tempranas en la vida, véase por ejemplo: Woolf, M., "Failures' targeted at birth", *The Independent*, 16 de julio de 2006, <http://news.independent.co.uk/uk/politics/article1180225.ece>.
- <sup>75</sup> La llamada "biocriminología" o los aspectos genéticos del comportamiento delictivo están disfrutando de un interés renovado en la actualidad; véase, por ejemplo: Rose, D. (2006) "Lives of crime", *Prospect* 125

(agosto), [http://www.prospect-magazine.co.uk/article\\_details.php?id=7604](http://www.prospect-magazine.co.uk/article_details.php?id=7604). Para leer una crítica previa a este enfoque, véase: Rose, N. (2000) “The biology of culpability: pathological identity and crime control in a biological culture”, *Theoretical Criminology*, 4 (1), 5–34.

<sup>76</sup> En 2016, la cárcel es ahora simplemente otro nivel de PCP. Los trabajos sociales, la libertad condicional y el encarcelamiento son todos un único continuado y fundamentalmente gestionado por empresas privadas.

<sup>77</sup> Supuestamente con la finalidad de mejorar la seguridad de los residentes, en 2010 se levantó una verja entorno a la barriada Dobcroft, dejando únicamente cuatro entradas y salidas, que son controladas por los Agentes de apoyo comunitario, cámaras y escáneres RFID.

<sup>78</sup> Este programa se introdujo de modo experimental en Shoreditch en Londres en 2006. Se le apodó de inmediato como “TV ASBO”, véase por ejemplo: Swinford, S., “Asbo TV helps residents watch out”, *Times Online*, 8 de enero de 2006, <http://www.timesonline.co.uk/article/0,,2087-1974974,00.html>.

<sup>79</sup> Véase el editorial del *New York Times*: “The data-fleecing of America”, 21 de junio de 2005.

<sup>80</sup> Véase Bennett, C. y Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, 2nd edn, Cambridge, MA: MIT Press.

<sup>81</sup> El registro de las actividades vitales o life logging es una evolución de los registros web. Ya se están desarrollando numerosas tecnologías para apoyarla; véase, por ejemplo: Ward, M. “Log your life via your phone”, *BBC News*, 10 de marzo de 2004, <http://news.bbc.co.uk/1/hi/technology/3497596.stm>.

<sup>82</sup> Véase el informe pericial Borders Expert Report y, por ejemplo, los vigilantes de seguridad fronterizos Minutemen en los EE.UU.: <http://www.minutemanproject.com/>.

<sup>83</sup> Esto ya ha sucedido en relación con el pánico creado en torno a los pederastas que en el año 2000 tuvo como resultado la expulsión de una pediatra de su propia casa; véase, por ejemplo: Allison, R., “Doctor driven out of home by vigilantes”, *The Guardian*, 30 de agosto de 2000, <http://www.guardian.co.uk/child/story/0,7369,361031,00.html>. Aquí simplemente se supone que en 2016, la tecnología permitirá que este tipo de errores circulen mucho más rápido y tengan un mayor ámbito de influencia.

<sup>84</sup> Ya abundan las guías para este tipo de resistencia; véase, por ejemplo: “Guide to Closed Circuit Television (CCTV) destruction”, *Schnews*, <http://www.schnews.org.uk/diyguide/guidetoclosedcircuittelevisioncctvdestruction.htm>.

<sup>85</sup> Véase Mann, S., Nolan, J. y Wellman, B. (2004) “Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments”, *Surveillance & Society*, 1(3), 331–355.

<sup>86</sup> RFID es una tecnología que requiere contacto visual directo. Se puede lograr causar interferencias mediante microondas, láminas de metal, ladrillos e incluso savia de árbol; véase, por ejemplo: “RFID Technology”, *RFID Centre*, <http://www.rfidc.com/docs/rfid.htm>.