

Un Informe sobre la sociedad de la vigilancia

Para el Comisario de Información

Para el Comisario de Información,
elaborado por la Red de Estudios sobre Vigilancia

Informe resumido

Septiembre de 2006

Editado por:

Kirstie Ball y David Murakami Wood

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

Introducción

En junio de 2006, el Comisario de Información del Reino Unido encargó a la Red de Estudios sobre la Vigilancia (*Surveillance Studies Network*) la elaboración de un informe sobre la sociedad de la vigilancia. Este documento constituye un resumen de dicho informe y consta de tres secciones en las que se tratan los aspectos esenciales del informe. En la primera, se presentan los componentes básicos de la sociedad de la vigilancia: sus definiciones, temas y repercusiones. En la segunda, se muestra cómo funciona la sociedad de la vigilancia. En la tercera, se examinan algunos de los retos que plantea la sociedad de la vigilancia en el ámbito normativo.

1. Sociedad de la vigilancia: resumen, historia, definiciones

Vivimos en una sociedad de la vigilancia. No tiene sentido hablar de la sociedad de la vigilancia en un tiempo verbal futuro. En todos los países ricos del mundo, la vida cotidiana está repleta de encuentros con mecanismos de vigilancia no sólo desde el alba hasta el anochecer sino durante las veinticuatro horas del día, siete días a la semana. No se trata simplemente de que las cámaras de CCTV capturen nuestra imagen cientos de veces al día o de que las cajeras desean ver nuestras tarjetas de fidelidad en el supermercado. Estos sistemas representan una infraestructura básica y compleja en la que se asume que la recopilación y procesamiento de datos personales resulta vital para la vida contemporánea.

Siempre ha existido alguna forma de vigilancia y las personas se han observado mutuamente, bien fuera para prestar asistencia, por motivos morales o para descubrir información de forma encubierta. Sin embargo, desde hace unos 400 años se empezaron a aplicar métodos “racionales” a las prácticas organizativas que eliminaron de forma paulatina las redes y controles sociales informales sobre los que se basaban previamente las prácticas comerciales y de gobierno habituales. Los vínculos sociales normales de las personas se hicieron irrelevantes, de forma que las conexiones familiares y las identidades personales no pudieran interferir con el funcionamiento idóneo de estas nuevas organizaciones, denominadas “burocracias”. No obstante, una consecuencia positiva de este cambio fue que los ciudadanos y, en última instancia, los trabajadores podían asumir que sus derechos serían respetados, ya que estaban protegidos por registros fidedignos y por leyes. La vigilancia se derivó de las prácticas impersonales y basadas en el seguimiento de normas. Las nuevas tecnologías de la información que aparecieron después de la Segunda Guerra Mundial revolucionaron la administración burocrática, mejorando su rapidez, grado de control y coordinación. Ello, junto con unas técnicas mejoradas de identificación y seguimiento desarrolladas en los departamentos militares y policiales, constituye el mensaje principal de este informe. La vigilancia aumenta a medida que la sociedad se va modernizando.

¿Qué tiene de malo la sociedad de la vigilancia?

La comprensión de la sociedad de la vigilancia como un producto de la modernidad nos ayuda a evitar dos trampas: concebir la vigilancia como una perversa conspiración urdida por poderes malignos o concebirla como únicamente el producto de las nuevas tecnologías (y, por supuesto, las personas de naturaleza más paranoica afirmarían que estas dos razones son en realidad una sola). Con todo, aunque se posea una perspectiva adecuada con respecto a la vigilancia, ello no quiere decir que no exista ningún problema. Lo que quiere decir es que debemos identificar las cuestiones fundamentales y hacer todo lo posible por llamar la atención sobre ellas.

La vigilancia tiene dos caras y debemos reconocer sus beneficios. No obstante, los sistemas a gran escala siempre presentan riesgos y, por supuesto, el poder corrompe o, por lo menos, distorsiona la visión de aquéllos que lo detentan. Las infraestructuras tecnológicas a gran escala tienden a sufrir problemas a gran escala. El pulsar de forma involuntaria o errónea un botón

puede tener fácilmente consecuencias catastróficas. Recordemos la publicación en agosto de 2006, por razones de “investigación”, de veinte millones de búsquedas en línea en AOL realizadas por personas corrientes. Supuestamente desprovistos de identificadores, sólo se tardó unos momentos en relacionar los registros de búsqueda con los nombres de las personas que las habían realizado.¹

También es necesario tener en cuenta la corrupción y las visiones distorsionadas del poder. De nuevo, para darnos cuenta de este problema no hay por qué imaginar un malvado tirano que obtiene las claves de acceso de bases de datos médicas o de la seguridad social. Un ejemplo de la corrupción del poder lo constituyen los líderes que apelan a un fin más elevado (por ejemplo, la victoria en la guerra) para justificar tácticas poco frecuentes o extraordinarias. En Estados Unidos, los ciudadanos estadounidenses de origen japonés fueron internados durante la Segunda Guerra Mundial gracias al uso (normalmente considerado ilegal) de los datos de censo. Más recientemente, se ha clasificado a muchos musulmanes estadounidenses no aptos para viajar mediante el uso de listas de exclusión de vuelo o se han creado perfiles raciales sobre los mismos, una práctica condenada en otros contextos por ser manifiestamente injusta.²

En el mundo de la alta tecnología y del comercio mundial abundan las consecuencias no previstas de acciones y políticas que en un principio contaban con las mejores intenciones. Por ejemplo, se nos dice que, para poder ser competitivas, las empresas “deben conocer a sus clientes” y, por consiguiente, dirigir su publicidad, e incluso ubicar sus fábricas y tiendas, de acuerdo con esos conocimientos. No estamos insinuando que el gerente de una tienda que desea atraer sólo a los clientes más solventes actúa ilegalmente al recurrir a los servicios de comprobación de crédito de Experian. Éste es un comportamiento lógico si se desea alcanzar una mayor rentabilidad. Pero los resultados (las consecuencias no previstas) de un análisis minucioso de los registros para crear una clientela rentable es que determinados grupos obtienen un tratamiento especial, basado en su capacidad de pago, mientras que otros son marginados.³

A un nivel más profundo, todos los procesos y prácticas actuales de vigilancia denotan un mundo en el que sabemos que no se confía en nosotros. La vigilancia fomenta la sospecha.⁴ 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 confía en 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. Se podría objetar que algunas de estas actividades simplemente demuestran un grado de prudencia. Sin embargo, ¿dónde se pone el límite? Las relaciones sociales se basan en la confianza mutua y si las socavamos de esta manera nos estamos abocando a un lento suicidio social.

¹ Véase: Barbaro, A. y Zeller, T. “A face is exposed for AOL searcher no. 4417749”, *New York Times*, 9 de agosto de 2006. <http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482/>

² Véase: Amnistía Internacional EE.UU. (2004) *Threat and Humiliation: Racial Profiling, Domestic Security and Human Rights in the USA*, Nueva York: Amnistía Internacional EE UU, http://www.amnestyusa.org/racial_profiling/report/rp_report.pdf

³ Lace, S (2005) *The Glass Consumer*, Bristol, Reino Unido: Policy Press; Danna, A. y Gandy, O. (2002) “All that glitters is not gold: Digging beneath the surface of data-mining” *Journal of Business Ethics*, 40: 373-386; Lyon, D. (ed.) (2003) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Londres y Nueva York: Routledge.

⁴ Esta cuestión se estudia en: Lyon, D. (2003) *Surveillance after September 11*, Cambridge, Reino Unido: Polity Press, págs. 45-48, 142 y sig.

La definición de la vigilancia; el análisis de la sociedad de la 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. El contacto cotidiano con la vigilancia incluye:

- Las cámaras de vídeo que 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 que 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) 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.

La vigilancia se encuentra dondequiera que observemos que se presta una atención con objetivos, rutinaria, sistemática y concentrada a nuestros datos personales con fines de control, concesión de derechos, gestión, influencia o protección. Analicemos esta frase por partes:

- La atención tiene *objetivos*; la observación puede justificarse en términos de control, concesión de derechos o cualquier otro objetivo acordado públicamente.
- Ocurre de forma *rutinaria*; se produce cuando realizamos nuestras actividades cotidianas.
- La vigilancia es *sistemática*; se lleva a cabo de acuerdo con un programa racional y no ocurre simplemente al azar.

- Por último, es *concentrada*. Gran parte de la vigilancia se refiere a personas identificables, cuyos datos son sometidos a procesos de recopilación, almacenamiento, transmisión, recuperación, comparación, minería y comercio.

Los detalles personales en cuestión pueden ser de diferentes tipos, como por ejemplo imágenes de CCTV, la biometría (huellas dactilares o reconocimiento de iris), los registros y contenidos de comunicaciones o, más comúnmente, los datos numéricos o categóricos. Debido a que una gran cantidad de datos son del último tipo y se refieren a transacciones, intercambios, extractos financieros, cuentas, etc., Roger Clarke ha denominado a esta categoría “vigilancia de datos” (en inglés, *dataveillance*).⁵ La vigilancia de datos se encarga de controlar o comprobar las actividades o comunicaciones de las personas de forma automática utilizando las tecnologías de la información. Resulta mucho más económica que la vigilancia electrónica directa o específica y, por consiguiente, ofrece beneficios que pueden actuar a veces como incentivos para ampliar el sistema, aun cuando los datos no se requieran específicamente para el objetivo original.

Perspectivas sobre la sociedad de la vigilancia 1: Procesos

A continuación haremos un inventario de los procesos y cuestiones relacionados con la sociedad de la vigilancia, tal y como acabamos de esbozar. De esta forma, ofreceremos un catálogo o lista de los aspectos importantes que se deben tener en cuenta a la hora de estudiar la sociedad de la vigilancia. Es necesario destacar que, aunque éstos varían en tiempo y lugar, todos ellos poseen una importancia crucial para la comprensión de los aspectos básicos de la sociedad de la vigilancia.

La *clasificación social* es endémica en la sociedad de la vigilancia. 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.⁶ 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.

El *flujo 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? Con el fin de proteger a los menores de abusos o reducir el fraude en los servicios públicos, a menudo se propone acudir a bases de datos cada vez más variadas. Sin embargo, el público en general y las agencias que comparten datos tienen conocimientos muy reducidos sobre dónde pueden acabar esos datos. Se ha impuesto la idea de que las intervenciones políticas deben basarse en datos de inteligencia y ello, junto con el potencial de conectividad y de comparación de datos que ofrecen las infraestructuras digitales actuales, hace que la vigilancia siga una lógica propia. Es necesario cuestionar, examinar y controlar esa lógica, en particular con respecto a aquellos procesos que implican el flujo de datos de un marco a otro.

La *desviación de uso* (en inglés, *Function Creep*) se produce cuando los datos personales, recopilados y utilizados para obtener un fin y satisfacer una función, se usan para otras funciones que intensifican las invasiones de vigilancia y privacidad más allá de lo que se asumió inicialmente y de lo que se consideró aceptable desde un punto de vista social, ético y jurídico.

⁵ Clarke, R. (2006[1997]) “Introduction to dataveillance and information privacy”, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV>

⁶ Véase el estudio clásico: Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information*, Boulder CO: Westview Press.

En el caso de las tarjetas Oyster en el Reino Unido, datos que en un principio formaban parte del ámbito comercial del transporte público se utilizan cada vez más en investigaciones policiales.⁷ La desviación de uso normalmente ocurre de forma sigilosa, en respuesta a una conveniencia administrativa. De hecho, debido a que las nuevas tecnologías permiten una cantidad cada vez mayor de intercambio de datos y debido a que la eficacia organizativa es considerada normalmente una prioridad absoluta, con demasiada frecuencia se desconoce, ignora o resta importancia a las consecuencias humanas de la desviación de uso.

Tecnologías: las tecnologías resultan críticas para la vigilancia, aunque es necesario tomar en consideración dos factores importantes: en primer lugar, la “vigilancia humana” de tipo directo, sin tecnología de por medio, aún ocurre y a menudo está ligada a tipos de carácter más tecnológico. En segundo lugar, los propios sistemas tecnológicos no son ni la causa ni la totalidad de lo que constituye la vigilancia hoy en día. No se pueden prever las consecuencias de la vigilancia cuando se analizan las capacidades de cada nuevo sistema. Para comprender adecuadamente la sociedad de la vigilancia, hemos de entender cómo funcionan las tecnologías, cómo se utilizan (este proceso es de carácter interactivo e incluye personal interno, consultores tecnológicos y operarios) y qué influencia ejercen sobre el funcionamiento de una organización. Por otra parte, necesitamos tener una idea clara de estas cuestiones para ejercer una influencia en las políticas y las prácticas, tal y como se indica en el análisis que realizamos más adelante de las evaluaciones de impacto.

Otra preocupación adicional con respecto a la tecnología es que un gran número de personas sostienen (erróneamente, como veremos más adelante) que es posible disipar la ansiedad existente ante la sociedad de la vigilancia a través de medios técnicos. No hay duda de que las llamadas tecnologías para la mejora de la privacidad (en inglés, *privacy-enhancing technologies*, PET) resultan útiles para frenar el crecimiento de la vigilancia tecnológica y se debería fomentar su uso cuando sea apropiado. Sin embargo, incluso en el mejor de los casos, éstas son solamente una parte de la respuesta. 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.

Perspectivas sobre la sociedad de la vigilancia 2: Temas

Privacidad, ética y derechos humanos: Desde la década de 1970 se ha reflexionado y debatido mucho desde un punto de vista jurídico sobre la vigilancia, lo que ha tenido como consecuencia la promulgación de leyes de protección de datos en Europa y leyes de privacidad en otras partes del mundo. Este tipo de normativa adopta una comprensión específica de la privacidad. Aunque los principios básicos sobre la protección de la información (en inglés, *Fair Information Principles*, FIP)⁸ han evolucionado, ha sido difícil convencer a los responsables de formular políticas de la importancia de las dimensiones *sociales* de la privacidad⁹, y menos aún de la necesidad de enfrentarse a problemas asociados con la sociedad de la vigilancia como tal. La sociedad de la vigilancia plantea dilemas sobre derechos éticos y humanos que trascienden el campo de la privacidad. No se debería esperar que las personas normales objeto de la vigilancia, por muy informadas que estén, tengan que protegerse a sí mismas. A continuación se exponen los tres temas claves en este ámbito:

Exclusión social y discriminación: 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, de igual modo, perjudicando a otros. La asistencia sanitaria y social desde el nacimiento hasta la muerte, que en el pasado constituía la promesa orgullosa de

⁷ Véase: “Oyster data use rises in crime clamp-down” *The Guardian*, 13 de marzo de 2006, <http://politics.guardian.co.uk/foi/story/0,,1730771.00.html>

⁸ Los FIP son el equivalente norteamericano de los “principios de protección de datos” europeos.

⁹ Véase el excelente estudio de los aspectos sociales de la privacidad en: Regan, P. (1005) *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill: University of North Carolina Press.

los gobiernos socialdemócratas, se ha visto reducida a una mera cuestión de gestión de riesgos y (en este punto es donde la sociedad de la vigilancia entra en juego) dicha gestión de riesgos requiere un conocimiento exhaustivo de la situación. Por ello, se busca la obtención de datos personales para determinar adónde dirigir los recursos.¹⁰

Elección, poder y concesión de derechos: 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? Cuando el sistema de vigilancia es inherente a la infraestructura y su funcionamiento está envuelto en un halo de misterio, resulta muy difícil 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.¹¹ 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 que procesan cantidades ingentes de datos de forma indiscriminada. Los individuos se encuentran en gran desventaja a la hora de controlar los efectos de la vigilancia.

Transparencia y responsabilidad: 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. No obstante, si tenemos en cuenta el poder de las grandes organizaciones con su sofisticada capacidad de vigilancia, parece justo que las personas corrientes deberían poder dar su opinión, aunque sólo fuera en relación a los principios. Es posible obtener información sobre esa opinión no sólo a través de agencias especializadas, sino también a través de grupos de presión y de los medios de comunicación.

Las organizaciones deberían asumir su responsabilidad, especialmente cuando se produce una vigilancia de gran intensidad de forma rutinaria con consecuencias potencialmente nocivas. Aunque la vigilancia del lugar de trabajo ofrece algunos ejemplos instructivos de prácticas incorrectas, al menos en algunos casos las empresas se han visto obligadas a frenar excesos de vigilancia gracias a la intervención activa de los sindicatos. Se pueden obtener resultados positivos mediante un proceso transparente en el que las empresas explican los detalles de la vigilancia y obtienen el consentimiento negociado de sus empleados. Sin embargo, cuando se trata de la vigilancia de los consumidores, no existe analogía alguna, a pesar de que el enorme poder de gestión de datos de Tesco o Walmart prácticamente no tiene paralelo. La aparición de la sociedad de la vigilancia actual exige que se produzca un cambio, pasando de la autoprotección de la privacidad a la responsabilidad de los manipuladores de datos. Esta tarea es análoga a los esfuerzos de los organismos reguladores para velar por el cumplimiento de los controles y ejercer presiones para reducir al mínimo la vigilancia.

¹⁰ Ericson, R. y Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.

¹¹ Véase el editorial de *New York Times*, "The data-fleecing of America", 21 de junio, 2005.

2. Un estudio de la sociedad de la vigilancia

La Red de Estudios sobre la Vigilancia encargó una serie de informes especializados en los siguientes ámbitos: la salud y la medicina; el consumo; el trabajo y el empleo; los servicios públicos; la ciudadanía; la delincuencia y la justicia; las comunicaciones; el urbanismo y la infraestructura; y las fronteras. De estos informes surgieron temas fundamentales que se pueden agrupar en cuatro áreas: el contexto de la sociedad de la vigilancia; las tecnologías de la vigilancia; los procesos utilizados por la vigilancia mediante los cuales se pone en práctica; y, por último, la forma en que la vigilancia afecta a los individuos y a los grupos en la sociedad. Por supuesto, estas áreas coinciden en gran medida en muchos casos, y existen otras áreas que no pudieron incluirse.

El contexto de la sociedad de la vigilancia

En primer lugar esbozaremos las diversas tendencias subyacentes en las sociedades occidentales que han desembocado en la sociedad de la vigilancia, a saber: el riesgo y la seguridad; la militarización de la vigilancia; y, por último, la creciente economía de la información personal.

El riesgo y la seguridad: Vivimos en una sociedad obsesionada por el riesgo. Las técnicas de gestión de riesgos que se ocupan de amenazas externas e internas se han convertido en una parte fundamental de las actividades organizativas. Se ha impuesto un enfoque *anticipatorio*, en contraposición a un enfoque *preventivo*.¹² De forma significativa, el uso de la minería de datos y de la elaboración de perfiles para identificar riesgos impulsa las prácticas de vigilancia hacia la investigación de las acciones y transacciones de la población general.¹³ Estas investigaciones se pueden utilizar posteriormente para concentrar las intervenciones en las personas o grupos de personas que se consideran expuestas a riesgos o suponen un riesgo para otros. La recogida y análisis de información, incluidos los datos sobre individuos identificables, resulta vital. De éstas se pueden derivar beneficios personales y sociales, aunque a la vez el concepto de seguridad tiene repercusiones importantes para la libertad, la privacidad y otros valores sociales, así como para la innovación y el cambio.

Algunos ejemplos ilustran esta tendencia hacia la gestión de riesgos y las medidas anticipatorias:

- La epidemiología y el modelado dentro de la vigilancia médica¹⁴ para identificar casos individuales, registrar incidencias para el análisis estadístico e identificar las categorías de la población que se encuentran en riesgo de contraer enfermedades específicas;
- La evaluación de riesgos de individuos, familias y vecindarios en la protección de menores, la salud mental y la justicia penal;
- La clasificación de los riesgos que los viajeros plantean a la seguridad nacional mediante el uso de manifiestos de pasajeros y transacciones financieras;
- La evaluación del valor relativo de los consumidores individuales y de sus perfiles geodemográficos.

La militarización de la vigilancia: La vigilancia militar es uno de los pocos fenómenos de los que se puede afirmar que son verdaderamente globales en una época en la que supuestamente todo se está globalizando. La Tierra está rodeada de múltiples satélites de vigilancia militar y los sistemas de vigilancia militar se han infiltrado totalmente en los sistemas de comunicaciones

¹² Ewald, F. (2002) "The return of Descartes' malicious demon: an outline of a philosophy of precaution", en Baker, T. y Simon, J. (editores), *Embracing Risk: The Changing Culture of Insurance and Responsibility*, Chicago: University of Chicago Press.

¹³ Valverde, M. y Mopas, M. (2004) "Insecurity and the Dream of Targeted Governance", en Lamer, W. y Walters, W. (editores) *Global Governmentality: Governing International Spaces*, Londres: Routledge.

¹⁴ Sobre la ascensión al poder de la economía de la salud, un campo que aplica exhaustivamente las técnicas y los resultados de la epidemiología a la evaluación de las tecnologías médicas, véase, por ejemplo: Ashmore, M., Mulkay, M.J. y Pinch, T.J. (1989) *Health and Efficiency: A Sociology of Health Economics*, Buckingham: Open University Press.

transnacionales. Con el Sistema de Posicionamiento Global (GPS) e Internet como dos ejemplos contemporáneos de tecnologías diseñadas con una capacidad militar integrada, es posible examinar paso a paso el desarrollo de toda la historia de la vigilancia moderna desde los avances iniciales basados en la Segunda Guerra Mundial y en los sistemas de Comando, Comunicaciones, Control e Inteligencia (C31) de la Guerra Fría, cuyo objetivo eran hacer del planeta un espacio totalmente defendible y seguro¹⁵. Esta interacción se manifiesta no sólo en los componentes tecnológicos y gubernamentales, sino también en nuestra forma de hablar, cada vez más militarizada, de la seguridad cotidiana: los medios de comunicación estatales y de masas hablan de la “guerra contra las drogas”, la “guerra contra el crimen” e incluso de la “guerra contra el terror”, de “leyes duras”, de “tolerancia cero”, etc. La “guerra de la información” ha emergido de la sombra oscura de las operaciones militares secretas a la luz brillante del mundo del comercio, en donde es común el espionaje industrial y los especialistas en penetración informática y seguridad se denominan ahora “guerreros de la información”. Un gran número de empresas tecnológicas de vigilancia están estrechamente vinculadas con el ejército y a la vez realizan ventas a usuarios civiles. Por ejemplo, TRW, un socio principal del contratista de defensa de EE.UU., se convirtió en una empresa líder en biometría en el ámbito civil; la empresa francesa Sagem fabrica todo tipo de dispositivos, desde teléfonos móviles hasta algoritmos de vigilancia para sistemas de reconocimiento aéreo sin tripulación.

La economía política de la vigilancia: Estas nuevas empresas, junto con proveedores de seguridad tradicionales y los grandes proveedores militares, forman parte de lo que se podría denominar, en líneas generales, la “industria de la seguridad”. Otros sectores industriales también son fundamentales para el crecimiento de la vigilancia, en particular las telecomunicaciones, la informática, la banca y los seguros. La industria de la seguridad se ha incrementado enormemente en los últimos años. De acuerdo con el índice de 100 empresas de la consultoría estadounidense *Security Stock Watch*¹⁶, el crecimiento de la industria en su conjunto ha superado constantemente los índices Dow-Jones y NASDAQ de alta tecnología¹⁷. A finales del año fiscal de 2005-6, el índice había aumentado más del doble en tres años, con una capitalización en el mercado aproximada para las 100 empresas incluidas en el índice de más de 400.000 millones de dólares estadounidenses.

Las economías de la información personal: No sólo los estados y organizaciones, sino también las personas corrientes, llevan a cabo actividades de vigilancia. Después del atentado terrorista de Londres en 2005, las cadenas de televisión y la policía instaron a los ciudadanos a que utilizaran las cámaras de sus teléfonos móviles para fotografiar a cualquier persona de apariencia sospechosa. Un número cada vez mayor de personas, en particular niños y jóvenes, exhiben los detalles de su vida (y a la vez observan las vidas de otros) a través de cámaras web en Internet¹⁸ y de sitios web de recreación social como *MySpace* y *Bebo*. Al mismo tiempo, todos aquellos que poseen un mayor acceso a los recursos de conocimientos están empezando a administrar su “doble de datos”, que se encuentran, por ejemplo, en las bases de datos de las agencias que proporcionan referencias de crédito, como por ejemplo *Experian* o *Equifax*. Estas agencias facilitan a las personas el acceso en línea a sus registros de crédito, permitiéndoles así cuestionar y corregir los datos que puedan inducir a error. No podemos depositar nuestra confianza en esta combinación de transparencia corporativa voluntaria y personas autodidactas como una forma válida de reglamentación, a pesar de que exista una nueva generación de jóvenes que están creciendo como ciudadanos habituados a llevar a cabo, ocuparse y ser objeto de actividades de vigilancia.

¹⁵ de Landa, M. (1991) *War in the Age of Intelligent Machines*, Cambridge MA: MIT Press; Edwards, P. (1997) *Computers and the Politics of Discourse in Cold War America*, Cambridge MA: MIT Press.

¹⁶ Este índice incluye los sectores de “biodefensa”, “seguridad medioambiental”, “prevención de fraudes”, “defensa militar”, “seguridad de redes de telecomunicaciones” y “seguridad física” (barreras, vigilancia por vídeo, etc.).

¹⁷ *SecurityStockWatch.com 100 Index*, agosto de 2006, <http://www.securitystockwatch.com/>

¹⁸ Koskela, H. (2004) “Webcams, TV Shows and Mobile phones: Empowering Exhibitionism”, *Surveillance & Society*, número especial dedicado a las cámaras de CCTV (editores Norris, McCahill y Wood), 2(2/3): 199-215, <http://www.surveillance-and-society.org/cctv.htm>

Las tecnologías de la vigilancia

Aunque resulta vital no olvidarse de la importancia de la vigilancia no tecnológica (por ejemplo, la escucha clandestina de conversaciones, el espionaje y la vigilancia que se sirve directamente de criterios humanos), esta sección centrará su atención en las cuestiones relacionadas con las tecnologías de la vigilancia. En primer lugar estudiaremos los progresos en cuatro áreas cuyos ámbitos coinciden parcialmente: las telecomunicaciones; la vigilancia por vídeo; las bases de datos; la biometría y las tecnologías de ubicación, control por medios electrónicos y seguimiento. Analizaremos la conexión entre las diferentes tecnologías y la tendencia que muestra la tecnología de la vigilancia de desaparecer y extenderse al mismo tiempo por todas partes. Concluiremos con un examen de los límites del desarrollo tecnológico.

El desarrollo tecnológico: Es incuestionable que las nuevas tecnologías han contribuido a cambiar la naturaleza de la vigilancia. Estos sistemas tecnológicos no poseen aspectos inherentes “buenos” o “malos”. Pueden utilizarse bases de datos nacionales eficaces para el suministro de una asistencia sanitaria específica o para la victimización de oponentes políticos. Sin embargo, tampoco se trata simplemente de qué uso se hace las mismas. Todas las tecnologías se desarrollan dentro de organizaciones específicas que poseen objetivos e intereses específicos. Examinaremos varias tecnologías específicas y sus capacidades.

Las telecomunicaciones: La vigilancia en el ámbito de las telecomunicaciones se refiere al grado en el que los individuos, las organizaciones y los órganos corporativos son capaces de controlar, clasificar y almacenar información sobre la ocurrencia y el contenido de los intercambios de telecomunicaciones, tanto entre los dispositivos tecnológicos como entre los dispositivos tecnológicos y las personas. Desde que el estado empezó la práctica de “intervenir teléfonos”, el desarrollo tecnológico ha tenido como consecuencia que se empleen tecnologías más diversas para las telecomunicaciones y una mayor capacidad de vigilancia. Por ejemplo, se puede determinar la ubicación de un dispositivo móvil mediante la simple triangulación de la señal del dispositivo con su recepción a través de una serie de estaciones base diferentes, a medida que las señales se van transfiriendo de una estación a otra, y esta información puede almacenarse para poder ser sometida a una minería de datos posterior. 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, filtra automáticamente de forma rutinaria todo el tráfico de telecomunicaciones que pasa a través del Reino Unido buscando palabras y expresiones clave, y emplea cada vez más algoritmos sofisticados para el reconocimiento avanzado del habla e incluso del significado¹⁹.

La vigilancia por vídeo: La vigilancia fotográfica ha existido desde finales del siglo XIX. Tras la ola más reciente de instalación de cámaras de CCTV en Gran Bretaña a partir de principios de la década de los 90, provocada por los intentos de contrarrestar el declive de los distritos de centros comerciales en las ciudades, además del miedo al terrorismo, es posible que este país cuente en la actualidad con hasta 4,2 millones de cámaras de CCTV: una por cada 14 personas,²⁰ y un mismo individuo puede ser filmado por más de 300 cámaras al día.²¹ Durante la década de 1990, el Ministerio del Interior británico (*Home Office*) se gastó un 78% de su presupuesto para la prevención de delitos en la instalación de cámaras de CCTV²² y se han invertido aproximadamente 500 millones de libras esterlinas de dinero público durante la última década en la infraestructura de cámaras de CCTV.²³ No obstante, un estudio del Ministerio del

¹⁹ Campbell, D. (1999) *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: Interception Capabilities 2000*, Luxemburgo: Parlamento Europeo, Dirección General de Investigación, Dirección A, El programa STOA; Wood, D (2001) *The Hidden Geography of Transnational Surveillance*, Tesis de doctorado no publicada, Universidad de Newcastle, Reino Unido.

²⁰ McCahill, M. y Norris, C. (2003), “Estimating the extent, sophistication and legality of CCTV in London”, en M. Gill (editor) *CCTV*, Perpetuity Press.

²¹ Norris, C y Armstrong, G. (1999), *The Maximum Surveillance Society: The Rise of Closed Circuit Television*, Oxford: Berg.:42

²² *ibid.*: 54

²³ Norris, C. (2006) “Closed Circuit Television: a review of its development and its implications for privacy”, documento elaborado para la reunión trimestral del Comité Consultor de la Integridad y Privacidad de Datos del Departamento de Seguridad Nacional de EE.UU. (*Department of Homeland Security Data Privacy and Integrity Advisory Committee*), 7 de junio, San Francisco CA.

Interior 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”.²⁴ La digitalización ha permitido el uso automático creciente de los sistemas de cámaras de CCTV. Hasta el momento presente, ello ha ocurrido principalmente en las carreteras. 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.²⁵ Este aumento en la vigilancia estatal ha recibido críticas sistemáticas en la prensa,²⁶ 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.²⁷ Existen planes para ampliar la capacidad del centro nacional de reconocimiento automático de matrículas (ANPR), que pasará de 35 millones de lecturas por día a 50 millones en 2008.

La base de datos: En la actualidad es posible recopilar, tabular y establecer referencias cruzadas entre datos múltiples de forma mucho más rápida y precisa que con los archivos de papel que eran en el pasado la característica distintiva de la burocracia moderna. Un nombre útil para la vigilancia que se sirve de bases de datos es “vigilancia de datos” (en inglés, *dataveillance*). Las bases de datos, combinadas con otros sistemas de vigilancia, también permiten la vigilancia algorítmica, el uso de software para tratar imágenes o datos capturados y su comparación con los incluidos en la base de datos. Este factor ha sido fundamental en el desarrollo de la biometría. La vigilancia de datos se utiliza exhaustivamente en los campos del marketing, la medicina, las actuaciones policiales y el control de fronteras.

Por ejemplo, en el *marketing*, a medida que se han reducido los costes de las bases de datos, muchas empresas del sector privado se han dedicado a recopilar el mayor número posible de datos sobre sus clientes y a concentrar sus actividades de marketing de forma más específica. Es posible combinar en la actualidad los datos de transacciones (el uso de tarjetas de crédito, las llamadas de teléfonos móviles, etc.) correspondientes a una persona con datos adicionales procedentes de programas de tarjetas de fidelidad, encuestas de clientes, grupos de sondeo, competiciones publicitarias, solicitudes de información sobre productos, contactos de centros de llamadas, *cookies* de sitios web, foros de reacciones de clientes y transacciones de crédito. Estos datos *internos* (que frecuentemente son propiedad de empresas privadas) a menudo están “recubiertos” con datos *externos* procedentes de agencias estatales (por ejemplo, estadística nacional), organizaciones sin ánimo de lucro o empresas especializadas en la recopilación de datos. Dichos datos se pueden asociar fácilmente con códigos postales, y determinadas calles reciben “perfiles” como “pensionistas prudentes”, “guarderías en ciernes” o “áreas industriales”.²⁸ Las técnicas sencillas de comparación de datos y la elaboración de perfiles geodemográficos se ven complementadas actualmente con sofisticados procesos “heurísticos” (de aprendizaje) en el campo de la minería de datos, a los que frecuentemente se denomina “descubrimiento de conocimiento en bases de datos” (*Knowledge Discovery in Databases*, KDD). De esta forma se pueden descubrir relaciones previamente desconocidas y *no obvias* dentro de conjuntos de información.²⁹ Tal vez la manifestación más clara del “producto” de

²⁴ Gill, M. y Spriggs, A. (2005). *Assessing the impact of CCTV*. Londres, Dirección de investigación, desarrollo y estadística del Ministerio del Interior británico (*Home Office Research, Development and Statistics Directorate*), 43, 60-61.

²⁵ Wilkins, G. y Addicott, 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.

²⁶ McCahill y Norris, 2003 *op cit.* n.44.

²⁷ 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

²⁸ La primera categoría (en inglés, *prudent pensioners*) se deriva del sistema de clasificación ACORN realizado por la empresa CACI, mientras que las otras dos (*fledgling nurseries* y *rustbelt resilience*) son clasificaciones MOSAIC de Experian. Se puede obtener más información sobre estos productos en <http://www.caci.co.uk/acorn/> y <http://www.business-strategies.co.uk/Content.asp?ArticleID=629>. Véase también: Burrows, R. y Gane, N. (de próxima aparición) “Geodemographics, software and class.” *Sociology*.

²⁹ Para obtener más información sobre las diferencias entre KDD y la minería de datos, véase Tavani, H.T. (1999) “KDD, data mining, and the challenge for normative privacy.” *Ethics and Information Technology* 1: 265-273. Muchas fuentes analizan la

estos sistemas sea la base de los sistemas de personalización en la web, como por ejemplo el utilizado por Amazon.com, el cual se sirve de fuentes múltiples de datos para pronosticar las preferencias probables de los compradores actuales.³⁰

Biometría: Todos los nuevos sistemas de identificación utilizan algún tipo de biometría: huellas dactilares, reconocimiento de iris, topografía facial y reconocimiento de manos son todos ellos utilizados en diferentes sistemas de tarjetas de identidad y pasaportes. El atractivo de la biometría es que parece proporcionar un “anclaje” de la identidad en el cuerpo humano al que es posible vincular datos e información. El identificador biométrico se convierte en la puerta de acceso a los datos almacenados. Se trata de lograr una convergencia de la minería de datos y de la integración de información con los identificadores biométricos. El objetivo es aumentar el grado de precisión y reducir las posibilidades de 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. La “guerra contra el terror” ha provocado un repentino aumento de la financiación de la investigación e implementación de la biometría. Después del 11-S en Estados Unidos se aceleró el desarrollo de las técnicas biométricas que ya se habían aplicado comercialmente o estaban a punto de ser utilizadas, y se las anunció como un factor clave para ganar este tipo de guerra.³¹ La llamada Ley Patriótica de Estados Unidos (*Patriot Act*), en un marco que tiene repercusiones que van más allá del suelo estadounidense, estableció un conjunto de prácticas para aplicaciones biométricas que ofrecían un uso casi ilimitado en la investigación e identificación de actividades terroristas. En el Reino Unido, la tendencia anteriormente mencionada hacia las cámaras de CCTV digitales ha tenido como consecuencia investigaciones adicionales en los aspectos prácticos de los sistemas de CCTV biométricos y del reconocimiento facial, tras la realización de experimentos iniciales en Newham, Birmingham y otros lugares.

Localización, seguimiento y control electrónico: Cada vez se utilizan más los Sistemas de Información Geográfica (*Geographical Information Systems*, GIS) para posibilitar la ubicación y organización de las prácticas de vigilancia, además de proporcionar referencias con respecto a las mismas³². Muchos de estos sistemas realizan un seguimiento de los movimientos geográficos de las personas, los vehículos o los productos mediante chips RFID (identificación por radiofrecuencia), Sistemas de Posicionamiento Global (GPS), tarjetas inteligentes de identificación, transpondedores o señales de radio emitidas por teléfonos móviles u ordenadores portátiles. Existen aplicaciones actuales de estas tecnologías en las esferas de los cuerpos y fuerzas de seguridad, la gestión de fronteras y el lugar de trabajo:

Por ejemplo, en el área de los *cuerpos y fuerzas de seguridad*, en 2004/2005 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.³³ 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)³⁴ o como una condición de su puesta en libertad condicional.³⁵

minería de datos como el proceso global de tratamiento de datos para los fines que se describen en este documento. Véase Rygielski, C., Wang, J-C y Yen, D.C. (2002) “Data mining techniques for Customer Relationship Management.” *Technology in Society* 24: 483-502, Danna y Gandy (2002) *op cit.* n.6. Por motivos de claridad, el término KDD se utiliza en el presente para definir el proceso técnico global que indica afinidades específicas (obvias o no obvias) dentro de conjuntos de datos, mientras que el término “minería de datos” se refiere a la práctica de acumular datos críticos para un análisis posterior de datos.

³⁰ 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.

³¹ Amoores, L. (2006) “Biometric borders: governing mobilities in the war on terror”, *Political Geography* 25: 2: 336-351; Gates, K. (2005) “Biometrics and post-9/11 technostalgia”, *Social Text* 23(2): 35-53. Irma Van der Ploeg, “Biometrics and the body as information”, in Lyon, D. (ed.) (2003) *op cit.* n.3.

³² *Institute for the Future* (Instituto para el Futuro) (2004) *Infrastructure for the New Geography*, Menlo Park, CA: IFTF.

³³ NPS (*National Probation Service*, Servicio Nacional de Libertad Condicional) (2006) *Electronic Monitoring* 6. <http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes>.

³⁴ 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

En el ámbito de la *gestión de fronteras*, en EE.UU. se están sometiendo a prueba las tarjetas inteligentes de fronteras habilitadas con RFID en la frontera entre este país y México. La industria de RFID apunta al potencial de esta tecnología para permitir el seguimiento durante un periodo limitado de tiempo de los trabajadores emigrantes que cruzan la frontera. Se están empezando a implantar chips RFID en los seres vivos, empezando por los animales. En EE.UU. también han sido implantados en 70 personas con enfermedades cerebrales degenerativas para poder realizar un seguimiento más fácil de las mismas³⁶ y una empresa ha implantado un chip en dos de sus empleados para controlar su acceso al *lugar de trabajo*.³⁷ Los avances continuos en la aplicación de datos geográficos en tiempo real a los perfiles de consumidores proporcionarán otra capa de datos para ayudar a las empresas a concentrar sus campañas de marketing en consumidores específicos. Por lo tanto, es muy probable que se produzca una “desviación de uso” de las funciones de estas tecnologías.

Sinergia tecnológica y desviación de uso: Aunque la capacidad de las tecnologías y sistemas individuales es significativa, cada vez se está produciendo más una sinergia o convergencia tecnológica de las tecnologías de vigilancia. Ésta es una tendencia a largo plazo dentro de los sistemas informáticos y también está motivada por el deseo de crear economías de escala. De forma creciente, los sistemas son diseñados teniendo en cuenta el objetivo de interoperabilidad entre los mismos. Ello también tiene como resultado que nuevos productos puedan emerger de viejas tecnologías (que ya habían sido comprendidas y gestionadas por los reguladores), combinándose para crear una función no regulada que no se había previsto. Por ejemplo:

- Tarjetas de identidad con diferentes funciones: el cruce de fronteras, el control del fraude, el acceso a la información gubernamental y quizás también un uso comercial (alquiler de cintas de vídeo) y semicomercial (bibliotecas). Cuando políticas como la “guerra contra el terror”, que ponen freno a la emigración de grupos no deseados e incluso a la búsqueda de soluciones para el fraude de tarjetas de crédito, están determinando el desarrollo de los sistemas de identificación, parece que se debilita un tanto el espíritu “impersonal” de la burocracia clásica.
- El ANPR (reconocimiento automático de matrículas) en Londres fue creado originariamente con objetivos militares y se instaló para ayudar a identificar a terroristas del IRA. En la actualidad desempeña una función en la gestión del tráfico, la recaudación de ingresos para la administración local y la seguridad contra una nueva generación de terroristas.

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. La informática omnipresente o ubicua (Ubicomp), también conocida como “inteligencia ambiental” (en inglés, *ambient intelligence*, AmI), crea las condiciones necesarias para una vigilancia omnipresente o ubicua al estar incorporada simultáneamente en los entornos físico y virtual.³⁸ Resulta relativamente fácil controlar los servicios y entornos electrónicos, en contraposición con las calles físicas y urbanas, aunque muchos puntos de paso urbanos incluyen actualmente componentes electrónicos y físicos que colaboran estrechamente entre sí. Se puede considerar la combinación de las cámaras de CCTV, la biometría, las bases de datos y las tecnologías de seguimiento como parte de una exploración mucho más amplia, a menudo financiada con el apoyo de la “guerra contra el terror” de EE.UU./Reino Unido, del uso de los sistemas inteligentes interconectados para realizar un seguimiento de los movimientos y

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 (*ibid.*: 6).

³⁵ NPS *op cit.*

³⁶ La empresa responsable es Verichip Corporation. <http://www.verichipcorp.com/>.

³⁷ Waters, R. (2006) “US group implants electronic tags in workers”, *Financial Times*, 12 de febrero. <http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html>.

³⁸ Kang, R. y Cuff, D. (2005) “Pervasive Computing: Embedding the Public Sphere,” *Washington and Lee Law Review* 62(1): 93-146. Cuff, D. (2002) Immanent domain: Pervasive computing and the public realm, *Journal of Architectural Education*, 57: 43-49.

comportamientos de millones de personas a través del tiempo y del espacio. En el lenguaje característico del sector, esto se denomina un seguimiento espacio-temporal multiescala.³⁹

Los límites de la tecnología: Por supuesto, las promesas hechas por las diferentes tecnologías casi nunca se cumplen tal como está previsto. Por ejemplo, las tecnologías biométricas para el programa USVISIT se redujeron de categoría por razones logísticas, pasando del reconocimiento de iris que se había planeado en un principio a las huellas dactilares digitales. También existen preocupaciones con respecto a su fiabilidad,⁴⁰ el “fallo de alistamiento” (en inglés, *failure to enrol*, FTE) (los datos biométricos son irreconocibles) y el “falso negativo” (en inglés, *false non-match*) (la lectura posterior no coincide con los datos biométricos individuales registrados). A pesar de ello, a menudo se toman decisiones fundamentales de implementación antes de llevar a cabo pruebas exhaustivas. Por ejemplo, en el sistema propuesto de tarjetas de identidad en el Reino Unido, se ha calculado que hasta una de cada seis personas tal vez no puedan utilizar sus carnés de identidad debido a problemas de FTE.⁴¹ También se han identificado problemas similares con tecnologías pertenecientes al ámbito de los cuerpos y fuerzas de seguridad, como por ejemplo el reconocimiento facial y el ANPR.

Dependencia tecnológica y retraso normativo: Normalmente se promueven las tecnologías de la vigilancia como “la mejor respuesta” ante múltiples amenazas, más recientemente la amenaza del terrorismo. Sin embargo, cuanto más nos comprometemos con las tecnologías de la vigilancia, más parece que existe una dependencia tecnológica (*technological lock-in*) con respecto a las mismas y menos posibilidades tenemos de estudiar otras opciones, y mayor es la laguna de comprensión que nos obliga a depender de expertos ajenos al sistema democrático. Los reguladores van constantemente a la zaga de la innovación tecnológica, incapaces de comprender su funcionamiento preciso. En esta persecución constante, hay que preguntarse si los estados poseen las herramientas necesarias para llevar a cabo una reglamentación útil de las prácticas de vigilancia complejas. La cuestión que se plantea con frecuencia con respecto al desarrollo tecnológico es si “se puede volver a meter al genio en la lámpara”. Los titulares de patentes y los vendedores suelen guardar silencio sobre la posibilidad de revertir los efectos de estos dispositivos y sistemas.

³⁹ Hampapur, A. et al. (2005), “Smart video surveillance”, *IEEE Signal Processing Magazine*, marzo: 38-51.

⁴⁰ Véase: Zureik, E. con Hindle, K. (2004) “Governance, security and technology: the case of biometrics” *Studies in Political Economy*, 73: 113-137.

⁴¹ Véase: Grayling, A.C. (2005) *In Freedom's Name: The Case Against Identity Cards*, Londres: Liberty.

Procesos de la vigilancia

La importancia de una evaluación preventiva de riesgos y la propuesta de la vigilancia como una solución a todo tipo de problemas ha dado lugar a una serie de procesos y fenómenos exclusivos a la misma. La clasificación social, las consecuencias no previstas, el intercambio de información y una diferenciación cada vez menos clara entre el ámbito público y el privado constituyen cuatro ejemplos de estos procesos.

Clasificación social, categorización y concentración. En muchas áreas se puede observar la clasificación social, es decir, la clasificación de la población en diferentes categorías según sus riesgos, valor o derechos:

- Los consumidores suministran continuamente a las empresas datos de transacciones y forman parte de un círculo de información que vincula el consumo con la recopilación de datos y la creación de perfiles.⁴² Los centros de llamadas en la actualidad clasifican las cuentas de clientes de acuerdo con su gasto relativo y prestan un nivel de servicio acorde a este gasto. El sector de telecomunicaciones registra los datos del tráfico para identificar las mejores rutas al mercado (por ejemplo, comercializando productos mediante mensajes SMS de teléfonos móviles);
- Los empleados de los centros de llamadas son evaluados, de acuerdo con factores sociales y de estilo de vida, para que se correspondan con los del segmento del mercado al que dirigen sus actividades.
- Es corriente observar en la actualidad en muchos puertos de entrada por tierra, mar y aire líneas de “vía rápida” para un cruce acelerado, por ejemplo el sistema ‘Privium’ del Aeropuerto de Schiphol en los Países Bajos, el cual utiliza el reconocimiento de iris en el control de pasaportes, evitando así que se produzcan colas largas.

Control no deliberado: La vigilancia no debería igualarse con el control social directo.⁴³ La intención de la vigilancia a menudo es simplemente gestionar el flujo eficiente y rápido de artículos, personas e información.⁴⁴ No obstante, lo que para una persona resulta “eficiente”, para otra quiere decir “control social”: éste es el caso en particular de los sistemas con un alto grado de personalización, como por ejemplo la recuperación de registros de identidad, los cuales se sirven de identificadores sistemáticos y únicos para cada ciudadano.⁴⁵

Intercambio de información: Para permitir la clasificación social, la información ha de ser precisa y fácil de obtener. En muchos países, incluida Gran Bretaña, existe la tendencia hacia unos servicios públicos más integrados y coordinados, a menudo a través de asociaciones y de una labor de equipo entre diversos organismos. Cada vez más, una variedad de acuerdos de asociación local reúnen a diversos organismos y profesiones, lo que permite concentrar los conocimientos y experiencias de todos ellos a la hora de proporcionar servicios más integrados a los ciudadanos.⁴⁶ Una consecuencia de este avance fundamental es que se cuestionan los límites que en el pasado servían para salvaguardar (aunque fuera de forma frágil) la privacidad y los límites de la vigilancia, con frecuencia desconcertando al público y a los proveedores de servicios sobre cómo se gestiona o debería gestionar la información personal.⁴⁷ Éste es el caso

⁴² Esta cuestión se estudia en detalle en: Elmer, G. (2004). *Profiling Machines: Mapping the Personal Information Economy*. Cambridge, MA: The MIT Press.

⁴³ Lianos, M. (2001) *Le Nouveau Contrôle Social: toile institutionnelle, normativité et lien social*. Paris: L’Harmattan-Logiques Sociales.

⁴⁴ Graham, S. y Wood, D. (2003) “Digitising surveillance: categorisation, space and inequality,” *Critical Social Policy*, 23: 227-248.

⁴⁵ Se puede acceder a un punto de vista crítico de un informático en: Clarke, R. (2006) “National identity cards? Bust the myth of ‘security über alles!’”, <http://www.anu.edu.au/people/Roger.Clarke/DV/NatID-BC-0602.html>.

⁴⁶ 6, P., Raab, C. y Bellamy, C. (2005) “Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part I”. *Public Administration* 83 (1): 111-133; Bellamy, C., 6, P. y Raab, C. (2005) “Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part II”. *Public Administration* 83 (2): 393-415.

⁴⁷ En un documento de consulta reciente del *Home Office* se solicitan facultades adicionales contra el crimen organizado y los delitos financieros, sosteniendo que “el intercambio de datos con otras partes del sector público es bastante irregular, mientras que rara vez se realiza un intercambio de datos entre los sectores público y privado”. Se hace un llamamiento para mejorar los flujos de

de los servicios públicos, los cuerpos y fuerzas de seguridad, la gestión de fronteras y el marketing. Por ejemplo, más del 50% de la población del Reino Unido posee una tarjeta de fidelidad Nectar, operada por Loyalty Management UK. Existen 216 compañías de catálogo en el Reino Unido suscritas al consorcio de intercambio de datos Abacus, que cuenta con información sobre 26 millones de consumidores individuales, mejorado por Lifestyle Universe de Claritas. De esta forma se combinan datos sobre los ingresos, el estilo de vida y las etapas de la vida a nivel individual para cada uno de estos clientes.⁴⁸

La desaparición de los límites entre lo público y lo privado: Aunque los sectores público y privado comparten información, los límites entre los intereses de los sectores estatal y privado se están haciendo más borrosos, a medida que un número cada vez mayor de tareas del gobierno se llevan a cabo mediante la combinación, a menudo compleja, de mecanismos públicos, privados, del sector voluntario y del mercado. Cada vez más, una serie de acuerdos de asociación local reúnen a una variedad de organismos y profesiones, permitiendo así la concentración de sus conocimientos y experiencias en el suministro de servicios más integrados a los ciudadanos.⁴⁹ Cuando la información estatal está disponible para un uso privado, como se ha sugerido en el caso del Registro de Identidad Nacional (National Identity Register, NIR), hemos de plantearnos cuestiones sobre los límites del consentimiento de las personas en su calidad de ciudadanos y consumidores, y sobre donde se situarán exactamente esos límites. La privatización de las telecomunicaciones, de la gestión de fronteras (el proyecto Semáforo de IBM, el programa de fronteras electrónicas del Reino Unido) y de la seguridad local (por ejemplo, el Cuerpo de Ciudadanos (*Citizen Corps*) en EE.UU. que “presta atención a actividades fuera de lo común”) continuarán planteando otra serie de cuestiones.

Consecuencias sociales de la vigilancia

A continuación centraremos nuestra atención en las consecuencias sociales de las tecnologías y los procesos de la vigilancia que acabamos de analizar. Las críticas de la vigilancia normalmente se enmarcan dentro de los términos de la privacidad, y sin duda ésta es un área fundamental, aunque preferimos estudiar esta cuestión como un aspecto de la autonomía individual. También nos gustaría hacer hincapié en los resultados de la elección y el consentimiento, un debate frecuente; y lo que es más importante, los procesos de clasificación, categorización y concentración con respecto a las oportunidades en la vida de individuos y comunidades o grupos enteros, así como su movilidad relativa y su acceso a oportunidades.

Autonomía: anonimato y privacidad: La vigilancia afecta a la autonomía al comprometer el anonimato y la privacidad de las personas. En muchos sentidos, una condición general de anonimato permite a las personas dar forma a su identidad a través de sus acciones y relaciones. Una de las primeras víctimas de la vigilancia omnipresente, y en particular de los sistemas de identificación, es el anonimato que permitía a las personas escapar de las restricciones de una vigilancia humana intensa en las pequeñas comunidades. La privacidad de las personas vulnerables y marginadas disminuye constantemente. En las prisiones británicas, los presos son objeto de una vigilancia casi continua. Incluso cuando son puestos en libertad, los delincuentes están sometidos cada vez más a un seguimiento electrónico, ya sea como una condición de una puesta en libertad anticipada en virtud del programa de detención domiciliaria (*Home Detention Curfew Scheme*)⁵⁰ o como una condición de la puesta en libertad condicional.⁵¹ Se debe someter

información, incluidas (por lo que respecta a los informes de actividades sospechosas) la comparación de datos entre la nueva Agencia contra el Gran Crimen Organizado (*Serious Organised Crime Agency*, SOCA) y las bases de datos de una gran cantidad de organismos gubernamentales, entre los que figuran la Agencia Tributaria y Aduanera (*Her Majesty's Revenue and Customs*), la Agencia de Conductores y Matriculación de Vehículos (*Driver and Vehicle Licensing Agency*, DWP) y el Servicio de Pasaportes. Existen en la actualidad nuevas iniciativas, entre las que caben destacar el nuevo Comité Ministerial sobre el Intercambio de Datos (*Ministerial Committee on Data-Sharing*, MISC 31), que poseen competencias para “desarrollar la estrategia del gobierno en el campo del intercambio de datos en todo el sector público”.

⁴⁸ Evans, M. (2005) “The data-informed marketing model and its social responsibility.” en Lacey, S (2005) *op cit.*, n.3.

⁴⁹ 6 *et al.* 2005 *op cit.* n.24; Bellamy *et al.*, 2005 *op cit.* n.46.

⁵⁰ 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

a un escrutinio constante la capacidad de las empresas de hurgar en las vidas privadas de sus trabajadores. El hecho de que los sistemas de identificación nacional abarquen múltiples bases de datos, en particular bases de datos que se encuentran tanto en el sector público como el privado, es un tema muy preocupante. Asimismo, a finales de 2002 la BBC informó que los cuerpos y fuerzas de seguridad habían realizado más de 400.000 solicitudes de información de datos de tráfico a los operadores de redes de telefonía móvil.⁵² Como ha comentado la Unión para la Defensa de Libertades Civiles (ACLU) en su estudio de una nueva red de vigilancia, las empresas y ciudadanos “están siendo reclutados en la construcción de una sociedad de la vigilancia”.⁵³

Elección y consentimiento: El concepto de elección ha desempeñado un papel vital en los debates sobre la vigilancia y la protección de datos en Norteamérica. Sin embargo, en el Reino Unido no se le ha prestado tanta atención en comparación con otros medios de protección. ¿Es posible elegir entre ser vigilado o no, si se desea tener una vida normal? ¿Se puede seguir argumentando que hemos dado nuestro consentimiento a ser vigilados? Podemos observar un ejemplo práctico de la cuestión de la elección en el sistema de justicia penal. Nadie elige ser vigilado por las cámaras de CCTV según nos desplazamos por el espacio público, ni tampoco que los movimientos de nuestros vehículos queden registrados en el Centro ANPR de la ACPO (Asociación de Jefes de Policía). Las personas arrestadas no eligen suministrar huellas dactilares y muestras de ADN, sino que están obligadas a hacerlo, y éstas quedarán registradas permanentemente en la base de datos nacional de la policía, aun si se pone en libertad a los detenidos sin presentar cargos. Aunque no se puede forzar a una persona a suministrar una muestra de orina para comprobar la presencia de drogas, apenas existe elección en esta situación, ya que una negativa puede tener como resultado una multa, el encarcelamiento o ambos. Es prácticamente imposible que una persona sepa cómo se utiliza la información y cómo ésta puede, de forma sutil, afectar su vida; por ejemplo, al incrementar las posibilidades de que la policía detenga su vehículo o se le pida un pago por adelantado para obtener bienes y servicios. Una solución podría consistir en que las interacciones de la vigilancia estatal con los ciudadanos no sean obligatorias, si ello es factible. Éste es el enfoque propuesto para el carné de identidad en Gran Bretaña. Sin embargo, ésta es una solución ilusoria en gran parte, puesto que una vez que se necesite este carné para el acceso a una gama de servicios, se hará obligatorio *de facto*. Además, los medios de identificación actuales están relacionados con funciones únicas, como por ejemplo conductores, consumidores o turistas, mientras que el sistema de tarjetas de identidad proporciona al gobierno poderes para realizar un seguimiento de actividades en un abanico de funciones que no sólo incluyen todas las anteriores, sino también las funciones como ciudadano.

Discriminación: velocidad, acceso y exclusión social: La discriminación, que adopta la forma de diferentes velocidades, diferencias en la facilidad de acceso y diferentes grados de exclusión social, constituye un resultado importante de los procesos de clasificación social que se derivan de la vigilancia. La lógica gubernamental ha cambiado. Mientras que los antiguos conceptos de ciudadanía del siglo XX ponían el énfasis en la *inclusión* de todas las personas que reunían los requisitos necesarios en los sistemas de salud, asistencia social y protección jurídica, las nuevas prácticas de ciudadanía, incluidos los sistemas de identificación, parecen hacer hincapié en la *exclusión* de los grupos no deseados.⁵⁴ Las personas con acceso a recursos poseen una movilidad elevada (empresarios internacionales, turistas, etc.) y sus sistemas de identificación (desde tarjetas de crédito a tarjetas de viajeros frecuentes) contribuyen a acelerar su facilidad de movimiento. Sin embargo, para otros grupos por ejemplo, emigrantes con trabajo (o, peor aún, desempleados), refugiados o solicitantes de asilo, por no mencionar aquellas personas con un

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. Véase: NPS (2006) *op cit.* n. 82.

⁵¹ *ibid.*

⁵² “Phone firms ‘flooded’ by crime checks”. *BBC News*, 20 de diciembre de 2002, <http://news.bbc.co.uk/1/low/uk/2592707.stm>.

⁵³ Stanley, J. (2004) *The Surveillance-Industrial Complex*, Washington DC: ACLU.

http://www.aclu.org/FilesPDFs/surveillance_report.pdf.

⁵⁴ Bigo, D. (2004) “Globalized in-security: the field of the professionals of unease management and the ban-opticon,” *Traces*, 4.

nombre típicamente “árabe” o “musulmán”, estos mismos sistemas ponen muchas trabas a sus movimientos dentro de los países o entre países diferentes.

La intensificación de la vigilancia de la vida urbana también implica procesos importantes de exclusión social. Esta exclusión se caracteriza por el fomento de una falta de conexión para aquellas personas y lugares que no se consideran rentables o se consideran arriesgados en cualquier sentido. Por consiguiente, un aspecto crucial es que las nuevas tecnologías de vigilancia pueden *ralentizar* las vidas de determinadas personas, causándoles un número mayor de problemas logísticos. Una vez que se introducen estas medidas, se realiza una monitorización automática creciente del acceso y el bloqueo,⁵⁵ lo que supone el riesgo de una dependencia tecnológica (*technological lock-in*) que divide a las sociedades contemporáneas de forma contundente en dos clases, una clase conectada, de alta velocidad y alta movilidad, y otra clase desconectada, de baja velocidad y baja movilidad. También se puede observar una exclusión en la estructura de los precios de los artículos. Por ejemplo, Amazon.com vende a diferentes clientes los mismos DVD con un precio diferente, por lo que se plantea la cuestión de si es necesaria una intervención reguladora para garantizar que no se produzca una fijación comercial de precios en masa. Aunque es difícil sacar conclusiones sobre la vigilancia en el lugar de trabajo y su relación con la exclusión social, principalmente debido a los factores determinantes estructurales sociales y ocupacionales preexistentes, existe un área en la que se están empezando a estratificar las oportunidades de empleo: el reclutamiento electrónico. Cuando se examinan grandes volúmenes de currículum vitae y se buscan posibles candidatos, se plantea de dos formas la cuestión de la discriminación. En primer lugar, debido a que el reclutamiento electrónico está sujeto a “reglas generales” y preferencias, que se plasman en la elección que realizan los profesionales de los términos de búsqueda de palabras clave,^{56 57} y en segundo lugar debido a que determinados grupos sociales, económicos y étnicos no poseen un acceso fácil a Internet.

Estos factores pueden pasar a formar parte de la propia infraestructura de la sociedad. Cuando el criterio humano es eliminado y enterrado en códigos informáticos, y cuando la identidad cultural y nacional se ha convertido en una dimensión disputada de la vida que tiene que soportar la pesada carga de oportunidades vitales y elecciones, recuerdos y esperanzas, resulta irónico que se realicen esfuerzos paralelos para reducir esta identidad a fórmulas y algoritmos legibles por ordenadores que faciliten una administración burocrática, policial y empresarial.

Democracia, responsabilidad y transparencia: Nos enfrentamos a muchas cuestiones en este campo: ¿Dónde se encuentran los límites del escrutinio público? ¿Cómo se reglamentarán los límites entre las bases de datos comerciales y la seguridad pública y estatal? ¿Cómo se conseguirá que las empresas privadas asuman su responsabilidad por los errores o resultados falsos en sus sistemas de bases de datos? Por ejemplo, los ciudadanos que se encuentran en una lista de vigilancia de “fronteras inteligentes” poseen en la actualidad un acceso muy limitado a la misma. Aunque un gran número de organismos y autoridades pueden acceder al sistema o introducir información en el mismo, existe una capacidad restringida de eliminar o corregir esos datos. Por último, se plantean cuestiones de considerable importancia sobre la responsabilidad de los gobiernos para con sus ciudadanos y la naturaleza “exterior” de muchos de los contratistas privados de los sistemas de vigilancia actuales. De hecho, los bancos de datos comerciales, como por ejemplo las transacciones de tarjetas de crédito o los registros de teléfonos móviles que están en poder de empresas multinacionales, pueden tener una base “exterior”, fuera del alcance directo de una jurisdicción política. Los ejemplos recientes de multinacionales que extraditan información plantearán retos específicos para la reglamentación

⁵⁵ Lianos, M. (2001) *op cit* . n.109; Lianos, M. (2003) “Social control after Foucault,” *Surveillance & Society* 1(3): 412-430. [http://www.surveillance-and-society.org/articles1\(3\)/AfterFoucault.pdf](http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf).

⁵⁶ Tversky, A. y Kahneman, D (1974) “Judgement under uncertainty: heuristics and biases,” *Science* 185(4157): 1124-1131

⁵⁷ Mohamed, A.A., Orife, J. y Wibowo, K. (2002) “The legality of key word search as a personnel selection tool,” *Employee Relations* 24(5).

y el escrutinio públicos, en particular cuando una empresa posee los datos comerciales y *a la vez* tiene un contrato para realizar funciones de vigilancia.

En virtud de la legislación de muchos países, los ciudadanos tienen derecho a conocer qué información se guarda sobre ellos y de qué forma se está utilizando la misma, aunque existen excepciones a este requisito. Este derecho exige que un “controlador de datos” proporcione a cada persona información sobre todos los datos existentes sobre la misma, así como detalles de cualquier procesamiento al que se ha sometido esta información. De esta forma se rectifica, hasta cierto punto, la desigualdad de poder existente en el mundo de la vigilancia, en particular cuando el consentimiento para el uso de nuestros datos personales es implícito y no se ha otorgado explícitamente. Con todo, un gran número de personas no conocen ni ejercen sus derechos, y apenas reciben ayuda si desean ejercerlos.

La intensificación de la vigilancia de datos se está convirtiendo en una característica normal del estado moderno que puede, en sí misma, ser justificable (y justificada por todos aquellos que la promueven) como una cuestión de interés público. Estas actividades a menudo pueden ser permitidas explícitamente por el parlamento. Lo que las convierte en actividades problemáticas es su manipulación de grandes cantidades de datos personales de una forma que excede los límites establecidos por los principios y las leyes de protección de datos (el parlamento, una vez más) y por otras restricciones y directrices sobre cómo recopilar, cotejar y comunicar la información. Es posible que nos acostumbremos, sin darnos cuenta, a ser vigilados y a que nuestras actividades y movimientos sean observados y anticipados, sin la posibilidad (sobre todo en los servicios públicos) de elegir nuestra inclusión o exclusión en esta vigilancia, o de comprender exactamente qué ocurre con nuestros datos. Puede que aceptemos como “razonables” limitaciones de privacidad que hubiéramos rechazado en otras circunstancias si nos hubiéramos puesto a analizar lo que significa ser un ciudadano. No se tiene la certeza de si la situación política permitirá, en última instancia, que los derechos de la privacidad puedan oponer una resistencia a las incursiones de las organizaciones gubernamentales realizadas en “interés público”, aun cuando el interés del público sea claro y de mayor importancia. Si la vigilancia ha de ser “proporcional”, muchos factores dependen de cómo se interprete ese término y de quién lo interprete. Muchos otros aspectos también dependen de las garantías que existan con respecto a los nuevos avances de naturaleza más intrusiva.

4. La reglamentación de la sociedad de la vigilancia

La vigilancia exige una reglamentación. Por “reglamentación” no queremos decir únicamente los dispositivos jurídicos para el control de sistemas y prácticas, sino también cualesquiera técnicas que posean un efecto regulador⁵⁸: es decir, que apliquen normas a la vigilancia y al procesamiento de datos mediante la fijación de límites y controles. La mayoría de los sistemas para el control del procesamiento de datos personales han sido desarrollados en el contexto de la protección de datos con el objetivo de salvaguardar la *privacidad*. Nuestros comentarios en esta sección se refieren principalmente a estas estrategias. Sin embargo, la reglamentación de la *vigilancia* podría ser una cuestión diferente. Se podría argumentar que es necesario concebir la protección de la vigilancia en su propio ámbito, ya que sus efectos no deseados no incluyen sólo aquellos relacionados con la invasión de la privacidad, y que la primera línea de defensa, aunque no sea insignificante, es vulnerable. En esta sección del informe reflexionamos sobre la experiencia normativa y evaluamos si estas actividades son suficientes. También sugerimos posibilidades de mejora.

⁵⁸ Baldwin, R. y Cave, M. (1999) *Understanding Regulation: Theory, Strategy and Practice*. Oxford: Oxford University Press.

¿Qué problemas presenta la reglamentación?

La reglamentación de la privacidad y de la vigilancia se enfrenta a problemas comunes. Se pueden identificar al menos seis áreas de dificultad:

- La reglamentación ha sido normalmente de carácter reactivo: se ha proporcionado una respuesta a la evolución, la implementación y las prácticas tecnológicas después de que éstas se hayan producido.
- La reglamentación ha tenido un enfoque principalmente técnico y administrativo, basado en códigos de prácticas, el cumplimiento de requisitos jurídicos típicos y la aplicación de tecnologías de protección de la privacidad, dejándose únicamente un pequeño margen para la anticipación.
- Gran parte de la reglamentación se ha basado en una concepción limitada de la privacidad personal y de su valor sólo para los individuos, reflejando (forzosamente) las ideas actuales de los responsables de elaborar políticas, que con frecuencia poseen una visión restringida de lo que consideran el “interés público”.
- Se ha debatido y puesto en práctica la reglamentación sin haberla sometido, en gran parte, a un debate público. El debate ha tenido lugar dentro de las comunidades de expertos: por ejemplo, el mundo de la protección de datos o los cuerpos y fuerzas de seguridad. Por consiguiente, las personas normales han tenido una participación muy reducida en algunos de los temas más importantes de nuestra época.
- A menudo se considera la reglamentación, en términos políticos, como una carga impuesta injustamente sobre las empresas y el estado que pone trabas a la iniciativa, la toma de riesgos y la productividad. En Gran Bretaña se ha intentado llevar a cabo una liberalización, o “reglamentación mejorada”, para aligerar esa carga. Apenas existe un reconocimiento en la práctica de que las empresas y el gobierno pueden salir beneficiados de la mayor confianza pública y del rendimiento mejorado que se pueden derivar de la reglamentación, aunque sí que se ha hecho mención del mismo desde un punto de vista teórico.
- El debate en los medios de comunicación se concentra principalmente en las “historias de terror” sobre incidentes de invasión de privacidad, y también refleja visiones utópicas u “orwellianas” sobre las tecnologías de la vigilancia. Las noticias de interés periodístico son importantes, pero con demasiada frecuencia se hace caso omiso de las complejas cuestiones éticas y sociales relacionadas con la vigilancia. Cuando se somete a debate la vigilancia, a menudo se hace en términos simplistas de causa y efecto (“las cámaras de CCTV ayudan a prevenir la delincuencia”) o de miedo (“nos controlarán a todos”). De forma similar, las opiniones alternativas se refutan con el argumento falaz y peligroso de que “el que no tiene nada que ocultar, no tiene nada que temer”.

El estado actual de la reglamentación

La protección de la privacidad se ha extendido por todo el mundo durante, como mínimo, los últimos treinta y cinco años. Existen algunos principios emblemáticos sobre los que se fundamenta este desarrollo. De acuerdo con estos principios, se exige a las organizaciones que:

- sean *responsables* de la totalidad de la información personal en su poder;
- *identifiquen los objetivos* para los que se procesa la información en el momento de recopilación de la misma o con anterioridad a la recopilación;
- recopilen información personal únicamente con el *conocimiento y consentimiento* de las personas (excepto en circunstancias específicas);
- *limiten la recopilación* de información personal solamente a aquellos datos que sean necesarios para la consecución de los objetivos identificados;

- no utilicen o revelen información personal para fines diferentes a los identificados, excepto cuando cuenten con el consentimiento previo de las personas (principio de *finalidad*);
- *conserven* la información únicamente durante el periodo en que la necesiten;
- garanticen que la información personal se mantiene en registros *precisos, completos y actualizados*;
- protejan la información personal mediante *garantías de seguridad* apropiadas;
- sean *transparentes* con respecto a sus políticas y prácticas y no mantengan un sistema secreto de información;
- permitan a las personas sobre las que se recopilan datos el *acceso* a su información personal, con la posibilidad de modificarla si ésta es inexacta, incompleta u obsoleta.⁵⁹

Los reglamentos y normativas que regulan la invasión de la privacidad y la vigilancia, bajo la influencia de este conjunto o conjuntos similares de principios básicos sobre la protección de la información (Fair Information Principles, FIP), han adoptado la forma de leyes generales, leyes que abarcan determinados sectores (por ejemplo, las telecomunicaciones) o prácticas (por ejemplo, la comparación de datos) y documentos y declaraciones internacionales a nivel regional y mundial, de los cuales tal vez el más destacado sea la Directiva Europea sobre Protección de Datos (95/46/CE), así como la Directiva sobre la Privacidad y las Comunicaciones (2002/58/CE). Se han creado autoridades reglamentarias, como por ejemplo los comisarios de privacidad e información, a escala nacional, subnacional e incluso regional. Asimismo, las empresas privadas, las asociaciones comerciales y las autoridades públicas han formulado sus propios protocolos y códigos de práctica, y los comerciantes en línea han adoptado declaraciones o políticas de privacidad. En virtud de la normativa jurídica se han aplicado penas y sanciones a los delincuentes. En los últimos años, se ha conseguido el apoyo de las soluciones tecnológicas (las tecnologías para la mejora de la privacidad o PET) con el fin de limitar la recopilación de datos, proporcionar el anonimato y paliar el potencial de vigilancia de la propia tecnología. Los defensores de la privacidad han advertido claramente de los peligros existentes, han expuesto prácticas erróneas y han contribuido a una concienciación pública sobre cómo la vigilancia y la invasión de la privacidad puede afectar a nuestras vidas. Los medios de comunicación han respondido con frecuencia a las amenazas de la vigilancia, aun cuando esos propios medios obtienen beneficios económicos de la invasión de la privacidad de los famosos y de los ciudadanos “normales”.

La construcción de un sistema práctico para el control de la vigilancia sobre los frágiles cimientos de la protección de la privacidad de la información les parece a muchos una tarea infructuosa. Sin embargo, en opinión de otros⁶⁰, es posible extender la privacidad y su protección para abarcar otras situaciones (intrusivas desde un punto de vista físico) en las que existe una desigualdad entre los ciudadanos y los responsables de realizar esta vigilancia, por ejemplo en el caso de la vigilancia por vídeo. No obstante, las nuevas prácticas de la vigilancia comportan cada vez más discriminaciones y otros males sociales que arrojan consecuencias poderosas e injustas sobre las oportunidades y posibilidades de la vida de muchas personas, más allá del ámbito de las propias violaciones de la privacidad, las cuales tienen repercusiones principalmente en los individuos. Se puede argumentar, por consiguiente, que sea necesario replantearse y modificar (como mínimo) los regímenes normativos para la vigilancia y la privacidad con el fin de poder ejercer una influencia sobre el diseño, la puesta en práctica y las repercusiones de las nuevas tecnologías de la vigilancia, que son de naturaleza más intensiva y extensa. Con todo, la nueva vigilancia no trata sólo de las tecnologías. Se puede afirmar que el “problema” de los regímenes normativos no es sólo como hacer frente a las tecnologías, sino

⁵⁹ Bennett, C. y Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge MA: MIT Press, 12.

⁶⁰ Por ejemplo: Dubbeld, L. (2004) *The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance*. Enschede: Ipskamp Printpartners.

también cómo ejercer una influencia sobre las políticas y objetivos de aquéllos que las desarrollan y ponen en práctica, y cómo ejercer una influencia sobre las sociedades y pueblos sometidos a ellas.

Instrumentos reguladores: pros y contras

El repertorio actual de instrumentos políticos que se han utilizado en la privacidad y la protección de datos, y que por tanto son aplicables a amplias áreas de la vigilancia, se compone de:⁶¹

Instrumentos internacionales: La Convención Europea de los Derechos Humanos así como otras declaraciones internacionales aportan una fuerza jurídica y moral a la protección de la privacidad que puede desempeñar una función importante a la hora de poner freno a los excesos de la vigilancia. Éstos y otros documentos afines han dado forma a las actividades legislativas y de implementación específicas en un gran número de países y jurisdicciones más reducidas. Las actuaciones a nivel internacional son responsables en gran parte de la preeminencia del conjunto de principios que han regulado durante mucho tiempo la protección de datos, y por extensión, la vigilancia.

Leyes: La difusión mundial de la legislación para controlar el procesamiento de la información personal se ha producido con gran rapidez, desde sus principios en la década de 1970 hasta el momento presente. Muchos países han promulgado leyes generales y específicas a sectores para la protección de datos, y la mayoría de estas leyes han establecido tanto mecanismos específicos para garantizar el cumplimiento de las mismas como mecanismos de supervisión. Los segundos, en forma de comisarios de privacidad, resultan esenciales para salvaguardar la privacidad. EE.UU. continúa fuera del “club” de países con leyes exhaustivas en este ámbito, debilitando así los esfuerzos mundiales por reglamentar la vigilancia, que resultan por tanto de carácter poco sistemático e irregular. La falta de robustez de muchas leyes y de sus mecanismos de implementación en el campo del procesamiento de la información personal ha sido un motivo de queja durante mucho tiempo. Es posible que los críticos tengan razón al impacientarse con las soluciones jurídicas que legitiman la vigilancia, en vez de reglamentarla.⁶² Además, las leyes de privacidad y de protección de datos no reglamentan fácilmente una amplia gama de prácticas de vigilancia, como por ejemplo aquéllas que forman parte de las telecomunicaciones modernas, y no es posible ampliar su interpretación fácilmente para que lo hagan. Por otra parte, el daño que la vigilancia puede ocasionar a personas, grupos y sociedades enteras no se enmarca dentro de los límites del impacto que estas leyes, basadas en los derechos individuales, tienen como objetivo remediar o impedir.

Autorregulación: Las industrias o empresas, los organismos especializados y los estados han desarrollado una diversidad de códigos de conducta o práctica para regular la vigilancia en muchas esferas de actividad. También existen medios en línea para la autorregulación por parte de empresas que desarrollan sus actividades comerciales en Internet. Estos medios adoptan la forma de declaraciones de privacidad en línea, respaldadas por organizaciones que las garantizan. A veces se incluye la autorregulación en la legislación, como ocurre con la Ley de Protección de Datos de 1998 del Reino Unido y la Directiva sobre Protección de Datos de 1995 de la UE (95/46/CE). Se considera la autorregulación cada vez más como la mejor forma de reglamentación, dado el “fracaso” de las leyes y el clima de una menor reglamentación para las empresas que se desea fomentar.⁶³ Sin embargo, resulta difícil imaginar la existencia de códigos e instrumentos similares sin la existencia previa y paralela de leyes o instrumentos internacionales que constituyen la fuente de las propias normas y directrices encarnadas por dichos códigos.

⁶¹ Para obtener una tipología y un debate más detallados, véase *op cit.* n. 59: capít. 4-7.

⁶² Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill NC: University of North Carolina Press.

⁶³ Departamento de Comercio de EE.UU., Administración Nacional de Telecomunicaciones e Información (NTIA) (1997) *Privacy and Self Regulation in the Information Age*. Washington DC: Departamento de Comercio, NTIA.

Tecnologías para la mejora de la privacidad: Un avance muy importante que se ha producido desde principios de la década de 1990 ha sido la comprensión de que las propias tecnologías pueden proporcionar controles robustos de la vigilancia o la invasión de la privacidad. Por lo tanto, el potencial de vigilancia o no vigilancia de tecnologías específicas depende de su diseño e implementación. Así, el cifrado de datos personales, cuando estos datos son almacenados o se transmiten a través de dominios y otras demarcaciones, puede oscilar entre inexistente y muy fuerte, mientras que el diseño de las redes y el “código” del software pueden tener un efecto regulador importante.⁶⁴ El cifrado, la navegación anónima por Internet, los dispositivos de filtrado, los agentes inteligentes, las herramientas de preferencia de privacidad y otros medios similares pueden actuar como instrumentos que confieren poderes a las personas. Sin embargo, no está claro si por sí mismos constituyen soluciones robustas a las prácticas de vigilancia en línea.

Autoayuda individual: Ésta es otra categoría general de la reglamentación. En este caso, las personas controlan la divulgación de información sobre sí mismos, no sólo a través del uso de las PET u optando por estar incluidas o excluidas en determinados procedimientos de procesamiento de información, sino también a través del conocimiento, la concienciación y la observación cuidadosa de las prácticas de vigilancia y de las amenazas para la privacidad. Todos estos mecanismos se basan en que los ciudadanos posean el suficiente interés en la protección y en la existencia de un “capital cultural”: la capacidad y los medios necesarios para comprender lo que está ocurriendo, para oponer una resistencia adecuada a las intrusiones y para tratar de obtener una reparación o compensación, una vez que estas amenazas se han hecho realidad. En EE.UU., a falta de organismos reguladores o de supervisión, la autoayuda (que incluye, por ejemplo, las demandas judiciales) es el medio dominante de regular la privacidad; este modelo ha recibido muchas críticas. Otros sistemas de protección de datos se basan, hasta cierto punto, en que los particulares presenten quejas a los reguladores y actúen como informantes de primera línea sobre prácticas sospechosas.

Asimismo, consideramos importantes las actividades de los siguientes grupos y personas:

- los grupos de presión relacionados con la privacidad y la anti-vigilancia, los cuales (junto con determinados sectores de los medios de comunicación) realizan una campaña de concienciación pública sobre las cuestiones y peligros existentes, hacen un seguimiento de las situaciones y ejercen presión sobre los gobiernos y empresas que utilizan la vigilancia;
- los tecnólogos que diseñan sistemas de vigilancia e información, y cuya educación, formación y adhesión a los códigos de práctica pueden afectar el grado de concienciación de sus empresas y determinar las características de los productos;
- los investigadores académicos, cuyo trabajo puede sacar a la luz lo que está ocurriendo, explicar por qué ocurre y desarrollar y someter a prueba teorías sobre las funciones y la legitimidad de la vigilancia en las sociedades del pasado, del presente y del futuro, aportando así sus conocimientos y experiencias al debate público.

Problemas generales relacionados con los instrumentos

Tres de los problemas más importantes a los que se enfrentan las prácticas reglamentarias actuales tienen que ver con la *fragmentación* y la *coordinación débil*. Un problema está relacionado con los *instrumentos* principales; el otro tiene que ver con el farrago de *niveles* jurisdiccionales en los que se supone que la reglamentación ha de ser aplicada. Para ambos problemas, la dificultad estriba en que la reglamentación se tendrá que enfrentar al reto de una vigilancia potencialmente más unificada y global si las tendencias actuales persisten. Para ambos problemas, la cuestión es cómo mejorar esta situación. En otras palabras, ¿es posible utilizar el fuego para luchar contra el fuego? Si las fuerzas que tratan de ampliar la vigilancia

⁶⁴ Lessig, L. (1999) *Code and Other Laws of Cyberspace*. Nueva York NY: Basic Books.

están cada vez mejor integradas y coordinadas, ya sea en un país o a nivel internacional, ¿qué integración poseen los instrumentos y los niveles de actividad protectora que tratan de contrarrestarlas? El tercer problema consiste en cómo aplicar estos instrumentos a las repercusiones sociales de la vigilancia (y, quizás de forma especial, a la “nueva vigilancia”) más allá de la invasión de la privacidad, o cómo crear nuevas herramientas. Con respecto a estos tres problemas, aún es posible replantearse las diferentes normativas para intentar incrementar su coherencia y eficacia. También se puede aún estudiar las posibilidades de aplicar la evaluación del impacto en la privacidad y la evaluación del impacto de la vigilancia a cualquier nivel y dentro de cualquier campo, dominio o sector de aplicación. En este documento nos limitaremos únicamente a indicar este tema.

Opciones para una reglamentación futura

Evaluación del impacto en la privacidad: Creemos que puede ser ventajoso adoptar el enfoque de la evaluación del impacto en la privacidad (en inglés, *privacy impact assessment*, PIA) en las prácticas reguladoras de las jurisdicciones a cualquier nivel que resulte pertinente.⁶⁵ La mejor forma de considerar la PIA es como un instrumento que aquéllos que proponen sistemas nuevos o revisados de procesamiento de datos pueden utilizar para paliar los efectos potencialmente nocivos en la privacidad en los sujetos. La PIA puede ayudar a mostrar cómo la protección de la privacidad puede tener cabida en un programa de intercambio de información como un requisito ético y jurídico que contribuye a objetivos sociales y políticos importantes, tales como una seguridad o unos servicios públicos mejorados y más orientados hacia los ciudadanos, y cómo esta protección de la privacidad no representa un obstáculo para dichos objetivos.

De la evaluación del impacto en la privacidad a la evaluación del impacto de la vigilancia: Para englobar los efectos potencialmente nocivos de la vigilancia en un ámbito más amplio que el de la protección de la privacidad, proponemos que sería necesario desarrollar herramientas de PIA que trasciendan la configuración existente y desarrollar lo que se podría denominar una *evaluación del impacto de la vigilancia* (en inglés, *surveillance impact assessment*, SIA). Ello, por supuesto, implica un cambio de significado, porque mientras que la PIA evalúa el impacto *del procesamiento de la información en la privacidad*, la SIA evalúa el impacto *de la vigilancia en una gama de valores* que pueden incluir, aunque también trascender, la propia privacidad.

Debido a que la PIA ha sido creada como una herramienta para estudiar la *privacidad*, concebida en términos de derechos individuales, en el momento presente no resulta el medio más apropiado para comprender las ramificaciones adicionales de la vigilancia con respecto a otros impactos personales y sociales. Para ello se necesitaría un cambio de paradigma y pasar de considerar únicamente las repercusiones sobre las *personas*, como suele hacer la política de privacidad, a considerar el valor de la protección de la privacidad y de la limitación de la vigilancia en términos sociales.⁶⁶ La privacidad no es sólo un valor de las personas, sino que también resulta importante para la sociedad como una base para el bien común y para los valores que se consideran comunes, como la democracia, la confianza, la sociabilidad y una sociedad libre e igualitaria. Debido a que el valor de la privacidad trasciende a las personas, a todos nos concierne el derecho y la capacidad de las personas para proteger su privacidad. Éste es un valor colectivo en la medida en que representa un bien colectivo que no puede ser fragmentado, de cuya protección los individuos no pueden ser excluidos y que el mercado no puede proporcionar de manera eficaz.⁶⁷ Por esta razón, la SIA podría desempeñar una función valiosa al incorporar la PIA, aunque a la vez trascenderla, gracias a una gama de investigaciones cuyo objetivo sería evaluar el impacto de la vigilancia (o invasión de la privacidad) sobre la propia sociedad y sobre los otros intereses, no relacionados con la privacidad, de diferentes personas, categorías y grupos.

⁶⁵ Stewart, B. (1999) “Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies,” *Privacy Law & Policy Reporter* 5 (8): 147-149; se incluye un debate descriptivo de la PIA en Raab, C., 6, P., Birch, A. y Copping, M. (2004) *Information Sharing for Children at Risk: Impacts on Privacy*. Edimburgo: Scottish Executive.

⁶⁶ Regan (1995) *op cit.* n.9, capít. 8.

⁶⁷ *ibid.*

Entre las cuestiones planteadas en una SIA podrían figurar:⁶⁸

- ¿Causa esta técnica daños físicos o psicológicos injustificados?
- ¿Traspasa esta técnica un límite personal sin permiso (ya implique una coacción o engaño, o un límite corporal, relacional o espacial)?
- ¿Viola esta técnica aspectos que se habían asumido sobre el tratamiento de la información personal como, por ejemplo, que no se pueden realizar grabaciones secretas?

Otras opciones: De la misma forma que la SIA continúa la labor de la PIA, existen otras opciones que pueden continuar las labores que se realizan en el presente actual.

- Crear una reserva de conocimientos en el ámbito tecnológico para ayudar a los reguladores a mantenerse al corriente de los avances que se produzcan en este campo.
- Aconsejar a los administradores y tecnólogos sobre cómo diseñar y poner en práctica técnicas de vigilancia de forma responsable, prestando especial atención a la estrategia, los cambios organizativos, la formación de personal y la responsabilidad social.
- Volver a conceptualizar la privacidad como un valor social colectivo, en vez de un valor individual.
- Fomentar un debate público sobre la vigilancia que sea participativo y no condescendiente.
- Llevar a cabo evaluaciones independientes de los costes de la privacidad, la reglamentación de la vigilancia y el cumplimiento de las normas. Estudiar si estos costes resultan excesivos y si afectan negativamente a la innovación. Estudiar si están justificados en vista de los beneficios obtenidos de confianza pública y eficacia, teniendo en cuenta que la prueba de “justificación” dista mucho de ser adecuada y debería ser sometida a un escrutinio.
- Elevar el tono utilizado por los medios de comunicación para que puedan ir más allá de los tópicos, el sensacionalismo y el alarmismo.

Por último, deberíamos mencionar cómo se podría mejorar la reglamentación si se estudian la idoneidad de las relaciones y la interdependencia de tareas entre los sistemas reguladores a diferentes niveles, incluido el mundial, y entre diferentes tipos de participantes, incluidos los organismos reguladores y los grupos en la sociedad civil. Es necesario someter a debate hasta qué punto, por ejemplo, las relaciones de cooperación que se indicaron en la Directiva de la UE 95/46/CE han resultado útiles no sólo para velar por el cumplimiento de las normas, sino también para reunir información y concienciar sobre temas en el plano más amplio de las prácticas y tecnologías de la vigilancia. También se debe estudiar hasta qué punto existe una relación fructífera entre los organismos reguladores y los grupos de la sociedad civil cuando estos últimos llaman la atención de los primeros sobre temas importantes, les proporcionan información o conocimientos útiles y dan la voz de alarma en aquellos casos en que la reglamentación no resulta eficaz o cuando las prácticas empresariales y gubernamentales parecen estar extendiendo el ámbito de la vigilancia. Una cuestión que va más allá del ámbito de este informe es si es posible incluir a participantes con funciones independientes en el sistema regulador, al margen de los reguladores comprometidos con su labor y de los defensores acérrimos de la anti-vigilancia. Tal vez este informe pueda servir para ilustrar esta nueva función.

⁶⁸ Gary T. Marx, “Ethics for a the New Surveillance”, *The Information Society*, 14, 3, 1998: 174