La sociedad de la vigilancia, el nuevo instrumento de poder

Descripción

Vivimos inmersos en un auténtico proceso revolucionario en lo que concierne a la información. Las nuevas tecnologías -telecomunicaciones- avanzan imparables permitiendo obtener, procesar y almacenar datos de una manera ilimitada. Con ello, se ha producido la desaparición de las fronteras espaciales y temporales, así como la instauración de un nuevo modelo de sociedad -la Sociedad de la Información-, que supone una transformación del poder y del mercado.

LA SOCIEDAD DE LA VIGILANCIA

En este orden de cosas, el poder se transforma a través de un proceso de descentralización y disgregación multidireccional hacia todos los centros de obtención de información, pues las nuevas tecnologías lo han ido desplazando, a la vez que el poder va cediendo terreno a los poderosos sujetos privados. Nos encontramos ante una realidad incuestionable, y es que la información constituye el moderno instrumento de control social. En este sentido, la noticia, el conocimiento, los datos… en definitiva, la tenencia de información, ha dirigido o encauzado el crecimiento y desarrollo del Estado a lo largo de este casi finalizado siglo XX, desempeñando la función que en su momento tuvieron la tierra o el trabajo. El peligro que, para los derechos de los ciudadanos, supone la acumulación de datos, lo previo o imaginó la Constitución cuando en el art. 18.4º estableció que «una ley limitará el uso de la informática…».

Está claro cómo el avance en la investigación científica es sinónimo de desarrollo y enriquecimiento de los Estados. Éstos clasifican a sus descubrimientos como secretos, y así nace el espionaje como primera de las técnicas de vigilancia y obtención de información reservada o secreta. No obstante, la investigación sigue diferentes direcciones. La información que persiguen los servicios de inteligencia se mantiene en secreto para uso exclusivo de los Estados, mientras que el conocimiento científico o académico se divulga para que aumente el saber de la sociedad.

No hace muchos años, tras la guerra mundial, se hablaba de un Estado de vigilancia que se esforzaba por detentar el control sobre todos los ámbitos como instrumento de fuerza y de poder. Ahora, esta forma de Estado ha dado paso a la sociedad de vigilancia. Emerge un nuevo poder con enorme impacto en la sociedad, muy diferente al poder centralizado del Estado. El problema no reside tanto en las técnicas de vigilancia sino en el uso que se da a la información obtenida: el enorme valor económico de los datos personales conlleva gran interés por obtener información, violentando a menudo el derecho del ciudadano a la vida privada. De ahí la necesidad de fortalecer los mecanismos legales de protección.

Así, pues, la vigilancia sigue siendo un mecanismo de poder, pero ha ido cambiando la forma de su adquisición, ya que cuando es el Estado quien tiene en sus manos el poder, la información se obtiene a través de los servicios de inteligencia, mientras que con las nuevas tecnologías, que responden a la descentralización y disgregación del poder, los datos se aportan voluntariamente por los vigilados. En un principio, la información que se obtiene se almacena en las bases de datos que se encuentran en manos del gobierno o de empresas, con fines institucionales específicos, pues los datos que se recogen y archivan corresponden a cuestiones muy determinadas. Las bases de datos (donde la recopilación, almacenamiento y recuperación está automatizada) rara vez contienen información obtenida de forma encubierta. De hecho, en el sector privado, el problema no es la obtención de información -recabada con el consentimiento de los ciudadanos- sino el uso que se hace de ella.

Al ser información obtenida de forma libre y consensual, se considera un producto comercial que puede y debe venderse para obtener beneficios, a diferencia de lo que ocurre con los datos obtenidos por los servicios de inteligencia que trabajan para el gobierno y se mueven en el más puro secretismo. No obstante, tanto los informes de unos como de otros, contienen información de carácter personal relativa a los ciudadanos (vigilados a través de varios ojos) que se destina a un uso concreto público o privado, con objetivos estatales o comerciales.

EL CONTROL PÚBLICO DE LA VIDA PRIVADA

En el mundo empresarial, es la estructura informativa de las bases de datos la que realiza los cálculos y predicciones, decidiendo, en base al resultado obtenido, quién merece ser excluido o quién es un cliente potencial de la empresa. Se produce así una clasificación de los ciudadanos, lo que conduce inevitablemente a una nueva clase social que responde a la que, por sus características o datos personales, es rentable para las empresas y gozará de los beneficios que éstas reportan. Las empresas e instituciones gubernamentales asumen una gestión basada en gran medida en el riesgo, y es el conocimiento de datos personales el que les sirve para catalogar a los ciudadanos e insertarlos en la categoría de incluidos o en la de excluidos, lo que supondrá la posibilidad de participar o no en un segmento de la economía y de la sociedad.

Una vez recopilada y almacenada la información personal, se abre el proceso de comercialización. Los datos de diferente naturaleza se comparan, se relacionan y amplían. Por ejemplo, una compañía de seguros puede buscar coincidencias con los archivos médicos para decidir sobre los seguros a negociar, lo que se traduce en la inclusión o exclusión de clientes potenciales. Por ello, si bien el poder está disperso y las bases de datos son muchas y variadas, cuando entran en relación con sus intereses comerciales se obtiene un intercambio de datos, por lo que el vigilante crece en su poder informativo.

De la ampliación de los datos obtenidos acaba resultando la transparencia absoluta de la vida de los ciudadanos: se conoce cuántos son en casa, cuál es la renta familiar, si viven de alquiler o en una vivienda propia, si tienen coche y de qué clase es el seguro, dónde van de vacaciones, qué les gusta comer y cuánto dinero gastan en manutención, los gustos y aficiones, la ropa que se compran y la marca del gel que usan en la ducha.

Pensemos por un momento en las numerosas técnicas de vigilancia que utilizamos sin valorar las desventajas indirectas que su uso supone para nosotros: tarjetas de crédito, cajero automático, tarjetas de salud inteligentes, etiquetas electrónicas, vigilancia videográfica, el auge y la

transformación de los medios de comunicación que se van especializando(con la consiguiente selección de consumidores). No sólo es la publicidad la que se dirige a determinadas audiencias, los medios de comunicación son también empresas de tendencia ideológica. En definitiva, la sociedad funciona a todos los niveles dirigida por el conocimiento de sus ciudadanos.

Internet merece una mención aparte como el más poderoso de los instrumentos de vigilancia, que abastece de información a los nuevos poderes de la sociedad de la información, y es que los ordenadores y las nuevas tecnologías de la comunicación reestructuran los modos de producción y de servicios: menos trabajadores, mayor flexibilidad laboral, más consumo y más mercadotecnia orientada al mismo. El acceso a Internet y la utilización diaria del correo electrónico son dos formas de obtener datos personales de los consumidores, quienes no reparan en el precio que han de pagar por encender su ordenador personal.

Un ejemplo del valor económico de la información personal se aprecia al ver cómo el mercado, tras comprobar el potencial del mundo *gay*, ha diseñado una campaña específica que se dirige a este colectivo. El estudio de sus gustos, tendencias y aficiones proporciona datos e información de carácter personal que, mal utilizada, puede servir para mostrar los peligros de esta vigilancia. En Estados Unidos, en 1998, un oficial de la Marina fue despedido a consecuencia de su homosexualidad. El oficial se había declarado homosexual en un formulario del proveedor de servicios de Internet mientras mantenía correspondencia electrónica y, a pesar de no identificarse personalmente, la Marina se enteró a través del proveedor y le despidió.

EL CONTROL PRIVADO DE LO PÚBLICO

No obstante, hemos de poner de manifiesto que la vigilancia a través de las altas tecnologías ha supuesto no sólo que los ciudadanos resulten vigilados -aumentando el control jerárquico de arriba a abajo- sino también a la inversa, pues los ciudadanos también se sirven de las tecnologías de la información, por ejemplo al grabar con una videocámara de vigilancia abusos policiales. Esto significa que la opinión pública tiene una forma de controlar el poder: la *contravigilancia* de los ciudadanos al poder político, que pone de manifiesto el efecto de vigilancia multidireccional. Aún recordamos los escarceos sexuales del presidente Clinton con su ex becaria, un asunto en el que se constata la vigilancia de los medios de comunicación sobre los personajes públicos, pues salió a la luz por las cintas grabadas de una conversación de carácter privado.

La contravigilancia se inspira en la idea de que la solución para defender la intimidad de los ciudadanos vigilados reside en las barreras que se imponen desde la ley y también en aquellas otras de carácter ético o moral, como son los códigos deontológicos: comisiones y códigos voluntarios en el sector privado o dispositivos legales para bloquear y controlar el trasiego de información. Esto presenta, sin embargo, una contradicción, pues se reclama mayor libertad de información y al mismo tiempo mayor protección de la intimidad. Se pide más seguridad, pero se quiere menos vigilancia.

GRAN HERMANO

Las tecnologías de vigilancia y represión son utilizadas a su vez por el Estado, quien controla, a través de bases de datos, los problemas que preocupan a los Estados en la actualidad, como la emigración y los movimientos de refugiados.

George Orwell creó el concepto de Gran Hermano en 1984, imaginando un monstruo que siempre nos

vigila como un gran tirano político. Tal como escribió Rusell Baker en el *New York Times*, en 1998, «la vigilancia no se limita a las autoridades oficiales como el FBI, el fiscal Kenneth Starr o el polícia local con su pistola radar. Hubo una vez un ciudadano privado que, con su cámara de videoaficionado, filmó a la policía de Los Angeles pegando a Rodney King. Actualmente hay cámaras de este tipo por todas partes; si se hurga la nariz, puede acabar saliendo en el *National Inquirer*; si en su patio trasero azota a su desobediente hijo de cinco años, puede acabar pasándolo mal por abuso de menores».

Llama la atención la escasez de protestas ante la invasión de la intimidad por las nuevas tecnologías de vigilancia, quizá porque las recompensas que se obtienen con el uso de estos avances de la ciencia inclinan a los ciudadanos a su aceptación.

No podemos olvidar la repercusión que una variante del concepto de Gran Hermano ha tenido como fenómeno televisivo, que consiste en que un grupo de personas viva las veinticuatro horas del día sometidos a una vigilancia total en una casa con paredes de cristal. A pesar de que hay voces contrarias a este tipo de programas, lo cierto es que la aceptación de la audiencia ha sido espectacular. Los habitantes de esa casa de cristal aportaron algo muy concreto a los espectadores: satisficieron la curiosidad por saber lo que ellos hacían en cada momento. Las ventajas de someterse a una vigilancia televisada – fama, notoriedad, dinero- se contrapone con las enormes desventajas para los participantes que, durante y después del concurso, perdieron su anonimato y sufrieron el control continuo y despiadado de sus datos personales con fines comerciales, como las investigaciones periodísticas que se empeñaron en desenterrar la cara más oscura de todos ellos.

Está claro que la Sociedad de la Información, lejos de desaparecer, se consolida en el mundo desarrollado. ¿Qué ocurrirá cuando ya no tengamos dónde ocultarnos? Para que esto no ocurra, los esfuerzos se centran en el control legal de la utilización de las bases de datos.

ORDENAMIENTO JURÍDICO EN ESPAÑA

Las leyes de protección de las bases de datos y las comisiones de vigilancia se centran más en el sector público que en el privado, aunque son las bases de datos privadas las que están desplazando a las estatales, dado que los sujetos privados cuentan con más dinero que les facilita el acceso a las altas tecnologías y entran con más fuerza en el mercado de la información. Son los pequeños hermanos del sector privado los que recogen más datos personales de los ciudadanos. Cedemos información para no ser excluidos del manantial de bienes que permite al mercado ir concretando grupos sociales o colectivos y, a partir de ahí, la individualización de los ciudadanos según su consumo, gustos o preferencias.

El ordenamiento actúa para proteger al ciudadano frente a tan devastadora invasión de su privacidad, pero no sólo para proteger los derechos de los ciudadanos sino también porque la asunción de poder político por la esfera económica debilita al Estado. La educación, la seguridad y la justicia, entre otros, son bienes que van quedando en manos privadas en cuanto que son servidos por empresas no estatales, pero que sólo son proporcionados a aquellos que, en base a sus datos personales, han sido incluidos en su mercado de servicios.

Las nuevas tecnologías han supuesto una nueva forma de entender el derecho a la intimidad como derecho a controlar las informaciones, lo que se ha denominado libertad informática, que permite controlar el uso de los propios datos introducidos en un programa informático. Este será un deber restrictivo para el Estado, que no puede impedir el acceso del interesado a las bases de datos, pero

que sí tiene que guardar el secreto frente a terceros que no podrán conocer datos que no les afecten personalmente. La legislación de protección de los derechos fundamentales va avanzando en la garantía de los derechos de los ciudadanos, pero ha de evolucionar más para poder reaccionar frente al imparable desarrollo tecnológico. La L.O 1/1982, 5 de mayo, de Protección Civil del derecho al honor, a la intimidad y a la propia imagen, (art.7); L.O 4/1997, 4 de agosto, que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, en su art. 9 reconoce los derechos de los interesados que, además de ser informados de forma clara y permanente de la existencia de videocámaras fijas, tienen la posibilidad de ejercer sus derechos de acceso y cancelación de las grabaciones en que figuran. La Disposición Adicional 7ª considera como faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad, permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o su utilización para fines distintos de los previstos legalmente, así como la reproducción de las imágenes y sonidos para fines distintos.

La L.O 5/92, 29 de octubre, de Tratamiento Automatizado de Datos Personales, desarrolla la previsión constitucional del 18.4º con el objetivo de limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos de las personas (art. 1). Resulta aplicable a los datos que figuren tanto en ficheros automatizados públicos como privados y a toda modalidad de uso posterior incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado (art.2). Asimismo, los afectados a quienes se solicite datos personales deberán ser informados previamente de modo expreso, preciso e inequívoco, de la existencia del fichero, de la finalidad y de los destinatarios, así como de otros aspectos: del carácter obligatorio o facultativo de las respuestas; de las consecuencias de la obtención de datos o de la negativa a suministrarlos, de sus derechos de acceso, de la rectificación y cancelación; de la identidad y dirección del responsable del fichero (art.5). En el art.7 se mencionan los datos personales que gozan de especial protección que, lógicamente, son aquéllos que revelan aspectos tales como la ideología, creencias, religión, vida sexual, origen racial … y que, en todo caso, se podrán recabar con el consentimiento expreso del afectado. Para la seguridad del fichero y la garantía de los derechos de los ciudadanos, el responsable del soporte y quienes intervengan en el tratamiento de datos, están obligados al secreto profesional (art. 10). La cesión de datos, que enriquece el mercado de la información, sólo puede obedecer al cumplimiento de los fines previstos y si hay consentimiento del afectado, salvo que una ley prevea otra cosa o que sean datos recogidos de fuentes accesibles al público… (art. 11). Los ciudadanos tienen derecho a estar informados por el Registro General de Protección de Datos de la existencia de ficheros, su finalidad y la identidad del responsable, siendo una consulta de carácter público y gratuito (art. 13). Asimismo, pueden acceder a la información registrada en los ficheros (art. 14) y solicitar la rectificación o cancelación de los datos inexactos o incompletos (art. 15). En todo caso, la Agencia de Protección de Datos se encarga de velar por el cumplimiento de esta legislación, atendiendo a las peticiones y reclamaciones formuladas por los afectados e informándolos sobre sus derechos en materia de tratamiento automatizado de datos (art. 36).

El Tribunal Constitucional en STC 254/93, FJ 6º, concede el amparo por denegación por la Administración de información sobre existencia, contenido y finalidad de ficheros automáticos o bases de datos donde constan datos personales del interesado. El Alto Tribunal entiende que es «garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también… un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado

de datos, lo que la Constitución llama informática».

Los datos que quedan más protegidos en la regulación legal del tratamiento automatizado de datos personales son los que con su utilización pueden provocar algún tipo de discriminación, mientras que aquellos de carácter económico son más accesibles o transparentes. Ahora bien, todo lo relativo a la persona ha de ser protegido por el ordenamiento, pues un simple dato económico es susceptible de desencadenar una completa radiografía de la persona. La exposición de motivos de la L.O.R.T.A.D. distingue entre intimidad y vida privada. «El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto la privacidad a una amenaza potencial antes desconocida». La privacidad es más amplia que la intimidad y abarca «facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca, pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservada. Si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros apartados del art. 18 de la Constitución y por las leyes que lo desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo».

Si entonces Orwell temía al Estado controlador, nosotros hoy debemos temer a las grandes compañías y empresas que comercializan con nuestros datos personales, siendo éstos los sujetos ante los que nos hemos de proteger en la Sociedad de la Información. En este sentido, le corresponde al legislador regular esta situación de peligro para salvaguardar los derechos fundamentales, para lo que se ha de encontrar el equilibrio entre la obtención de información y la protección de la privacidad.

Fecha de creación
29/11/2000
Autor
Ana Aba Catoira