Los archivos electrónicos en España: del Gran Hermano al control democrático

José Ramón Cruz Mundet.
Departamento de Biblioteconomía y Documentación
Universidad Carlos III de Madrid.

0.1. Resumen

El artículo analiza las consecuencias que traen consigo la extensión de los nuevas tecnologías de la información en España, en relación sobre todo a la privacidad de los ciudadanos. Trata de establecer además la situación que este hecho trae consigo en relación a la situación jurídica, y especifica también posibles consecuencias y soluciones a los conflictos que aparecen actualmente.

Palabras clave: Derecho a la privacidad. Tecnologías de la Información.

0.2. Abstract

The consequences of new information technologies on spanish citizens´ right to privacy are analyzed. The related legal aspects are considered, together with the possible legal consequences of current conflicts, and proposed solutions.

Keywords: Right to privacity. Information technologies.

1. Introducción

No sé muy bien por qué las referencias a las TI muestran una querencia sospechosa por los extremos:

- Uno de alucinada bobaliconería ante sus prodigios, similar al que se podía sentir tiempo ha con aquellos artilugios maravillosos con que los charlatanes de feria prometían solucionar los problemas cotidianos, herramientas que por cierto tambien eran diminutas, multiusos y de fácil manejo; pero que en la intimidad del hogar se desvelaban complejas, ingobernables y de escasa utilidad.
- El otro es negativo y obcecado ante lo nuevo, diferente y desconocido, bien arropada por la imaginería audiovisual, recuédese si no la serie televisiva de aquella simpática familia atrapada en el espacio por la inque-

brantable programación de un robot, la omnipotencia de Hall en 2.001 o el sistema de reserva de vuelo para Alien, el octavo pasajero.

La verdad es que no hemos inventado nada nuevo, pues ya hubo quienes concibieron un mundo atravesado por trenes que nos permitirían llegar a la luna, y otros que salieron al paso de los primeros con hisopo y jaculatorias queriendo fulminar con sus exorcismos a lo que parecía evidenciar el triunfo del Maligno en la tierra.

Así como aquellas premoniciones nos provocan una sonrisa burlona de superioridad, no me cabe duda de que nuestra ingenuidad provocará hilaridad en el futuro, sin embargo de lo cual merece la pena intentar analizar el estado de la cuestión.

2. El Gran Hermano

La necesidad de conocer unida a la capacidad tecnológica posibilitado una capacidad de control y vigilancia sobre la sociedad en general y sobre cada individuo en particular prácticamente ilimitado. Cada ciudadano español consta en más de 200 ficheros informáticos. Cuando nacemos se nos registra en el hospital, en la Seguridad Social y en el registro civil, por lo menos. Después somos inscritos en un colegio, ante la administración educativa, en el padrón municipal, nuestros datos pasan a poder de empresas mediante la participación en concursos y ofertas comerciales. Ya de jóvenes solicitar el DNI, el pasaporte o una beca, el ingreso en la universidad, el alistamiento militar, la pertenencia a alguna asociación o la suscripción a alguna revista, son motivos para ingresar en nuevos archivos informáticos. Con la edad madura abrimos cuentas, obtenemos tarjetas de crédito, solicitamos préstamos, sacamos el carnet de conducir, pagamos impuestos, nos casamos, nos divorciamos, compramos un coche, cambiamos de trabajo o nos vamos al paro, un buen día nos vemos envueltos en un juicio, somos fichados o, simplemente, la policía nos para en un control de carretera y recaba nuevos datos, suscribimos un seguro de vida...además de los años, se multiplica nuestra presencia en las bases de datos.

En sí mismo nada de esto es malo, ya que gracias a las posibilidades que ofrece la informática, la gestión de grandes organizaciones como la Seguridad Social o la Hacienda Pública han mejorado sustancialmente, la policía puede perseguir con más eficacia los delitos, las empresas saben más de nuestros gustos a la hora de ofrecernos sus productos y servicios, o con sólo teclear una clave podemos conocer el estado de nuestras finanzas y cómo gastamos nuestro dinero.

Sin embargo, el uso ilimitado de la informática puede llevarnos a resultados perversos. Es fácil entrecruzar datos de distinta procedencia sobre un individuo,

por ejemplo, hasta conseguir una imagen nítida que ni el propio interesado posee, e incluso una imagen falsa con la que hacerle la vida más difícil. Imaginemos qué pasaría si alguien pudiera obtener del banco al que hemos confiado nuestros datos, información acerca del movimiento de cuentas, del Ministerio de Trabajo datos sobre el salario, del padrón municipal los relativos al domicilio, convivencia, nivel de formación.., de la Seguridad Social sobre la salud, de Hacienda la relativa a las propiedades, y así un largo etcétera. Y si además de saber tanto sobre nosotros vendiera esta información nos encontraríamos prácticamente desnudos frente a terceros. Como vamos a tener ocasión de comprobar no se trata de un guión cinematográfico, sino de algo muy serio, tanto que nuestra Constitución recoge expresamente en su artículo 18.4 que "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*"

En enero de 1992 la policía irrumpía en la sede de la empresa Publicest y se incautaba del que entonces fue calificado como uno de los mayores y mejores bancos de datos de España, se trataba de 2.000 cintas magnéticas en las que constaban 53 datos diferentes -muchos de ellos reservados- relativos a cerca de 21 millones de españoles, más que los contenidos en *Berta* y *Duque de Ahumada*, los famosos ordenadores de la Policía y la Guardia Civil. Las informaciones, completas y muy precisas, habían sido obtenidas de manera fraudulenta de los ministerios de Interior, Trabajo y Seguridad Social y de Economía y Hacienda, así como de algunas empresas del sector bancario y automovilístico principalmente. El material, valorado en unos 1.000 millones de pesetas, permitía vender a otras empresas bases de datos a la carta que podían contener desde el domicilio, al salario, las propiedades, el saldo bancario y otros aspectos sensibles. Este caso, que fue muy sonado en los medios de comunicación, puso de relieve la inexistencia de una normativa legal y de medios ejecutivos para defender la privacidad frente a la utilización abusiva de la informática.

La privacidad es un concepto jurídico reciente de origen norteamericano, formulado en 1890 por Samuel D. Warren y Louis D. Brandeis, dos jóvenes abogados, en un artículo titulado *The Rigth to Privacy*. Originariamente era concebido como derecho de exclusión de los demás del ámbito privado, desde el que se ha pasado al actual de derecho a controlar los datos relativos a la propia persona que han salido del ámbito de la intimidad para formar parte de un archivo electrónico. Como señala la LORTAD (1992) en su exposición de motivos:

> "el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el

> domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo- la privacidad constituye un conjunto más amplio, más global, de 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 este tiene derecho a mantener reservado."

El concepto de privacidad contiene diversos elementos. Por un lado están los datos, distinguiendo los que están a disposición del público, de los denominados *sensibles*, relativos a la intimidad, a los comportamientos personales, a los elementos distintivos de la personalidad, a las opiniones religiosas y políticas.

Por el otro lo que ha dado en llamarse *habeas data*, la libertad de controlar el uso de los datos personales insertos en sistemas informáticos, que en la práctica se plasma mediante el ejercicio del derecho a: acceder a los bancos de datos para controlar la exactitud, puesta al día, rectificación y anulación de los datos de carácter personal, el derecho de secreto para los datos sensibles, y el derecho de autorización en cualquier caso para su difusión.

Todo esto que constituye el derecho a la privacidad suscitó desde muy pronto el interés de las democracias de nuestro entorno. En fechas tan tempranas como 1970, cuando el uso de los ordenadores estaba en una fase incipiente, el estado alemán de Hesse aprobó una ley de protección de datos (*Datenschutzgesetz*) en la que se instituía una magistratura independiente encargada de velar por su cumplimiento, era el Comisario para la protección de datos o *Datenschutzbeauftragter*. Así se establecía un modelo a partir del cual los países democráticos fueron adoptando medidas legislativas que ordenaran el uso de los datos personales por medio de la informática, acompañadas por la creación de organismos independientes a imitación del alemán. La magnitud del asunto y la sensibilidad social eran tales que en el caso de las jóvenes democracias, como la portuguesa y la española, se hace mención expresa en sus respectivas constituciones.

Por lo que hace a nuestro país aún se tardaron nada menos que catorce años en aprobar la ley correspondiente, la ya citada LORTAD:

- En parte inducida por la presión comunitaria en el sentido de crear un espacio europeo común también para la protección de datos,
- En parte por la eclosión sucesiva de diversos escándalos que evidenciaron el caos en que estábamos sumidos.

En julio de 1992, la Unión de Consumidores de España acusaba a Telefónica ante el Defensor del Pueblo por vender datos personales de sus abonados a empresas de publicidad directa. En efecto, la empresa Cetesa (filial de Telefónica) a través de su línea de negocio denominada Coditel, poseía datos

sobre la dirección y la situación económica de cientos de miles de españoles, los cuales vendía a la carta. Por ejemplo, por menos de un millón de pesetas se podían comprar direcciones de 100.000 personas de nivel económico medio-alto distribuidas en diversas ciudades españolas seleccionadas por el comprador. En una interpretación bastante laxa de las relaciones contractuales, la compañía aducía que salvo que se hiciera constar lo contrario en el contrato, Telefónica podía comercializar libremente los datos que sus abonados le habían proporcionado. Tesis en torno a la cual se alineó el Gobierno en noviembre, a pesar de haberse descubierto que esta era una de las fuentes de información de la fraudulenta empresa Publicest, desmantelada por la policía a comienzos de año. Gracias a la puesta en marcha de la LORTAD, la compañía se vio más tarde obligada a aprobar un código ético para garantizar el uso adecuado de los datos, en ningún caso fuera de la utilidad para la cual son cedidos.

Este es precisamente uno de los aspectos clave que recoge la legislación, la imposibilidad de utilizar los datos de carácter personal para fines distintos de los que han ocasionado su recogida y procesamiento. Esto supone, además, que no pueden ser comercializados, salvo que esa fuera la finalidad expresa, ni pueden ser intercambiados entre bases, mucho menos entre países, conocido como movimiento internacional de datos.

Otro de los focos de desprotección era el citado *habeas data*, la falta de control sobre la exactitud y actualización de los datos daba lugar a situaciones tan rocambolescas como la del diputado Enrique Curiel, quien en febrero de 1984 fue retenido durante 45 minutos en el aeropuerto de Barajas porque en *Berta* -el ordenador de Interior- constaba que se trataba de un peligroso comunista con numerosos antecedentes políticos por su militancia antifranquista. El error no hubiera existido de haberse cancelado con anterioridad los datos caducos, ni se hubiera repetido de haberse subsanado posteriormente; el caso fue que seis años más tarde en enero de 1990 en Frankfurt, la policía alemana retenía al diputado a causa de los datos proporcionados por sus colegas españoles. Los casos de ciudadanos anónimos fueron bastante frecuentes, según recogen las memorias anuales del Defensor del Pueblo al Parlamento, además de la prensa del momento, y demostraban su indefensión ante el uso de datos erróneos.

La paradoja era que las víctimas de la inexactitud documental no tenían siquiera la posibilidad de recabar los datos personales obrantes en poder de las administraciones y ejercer el derecho de rectificación y cancelación. Cuando el 28 de febrero de 1986, el diputado autonómico Francisco Javier Olaberri, invocando el artículo 18 de la Constitución, solicitó al gobernador civil de Guipúzcoa que le comunicara si algún organismo estatal poseía datos suyos de carácter personal y, en tal caso, le indicara la finalidad de los ficheros, la autoridad que los controlaba y los datos concretos sobre su persona; la respuesta fue

el silencio administrativo y un sinfín de recursos judiciales desfavorables, hasta que el Tribunal Constitucional en sentencia del 20 de julio de 1993 le amparaba en su derecho. Para entonces, afortunadamente, las cosas habían cambiado bastante desde el punto de vista legal.

A comienzos de ese año entraba en vigor la LORTAD, recogiendo los derechos de información y acceso, rectificación y cancelación, impugnación y exigencia de responsabilidades. Aunque básicamente garantiza el *habeas data*, la ley ha sido criticada desde muchos sectores por el trato discriminatorio que otorga a los ficheros de titularidad privada frente a los de titularidad pública, por cuanto éstos se benefician de múltiples excepciones al ejercicio de los derechos, invocando a veces argumentos tan difusos como *el interés general* para denegar el acceso a los datos personales. Lo más llamativo, como tendremos ocasión de comprobar, es que los ficheros con mayor cantidad de datos *sensibles*, sean precisamente los más difíciles de controlar.

3. El control democrático.

Siguiendo el modelo al uso se creaba pocos meses después la Agencia de Protección de Datos (APD), organismo encargado de velar por el cumplimiento de la legislación en la materia. Aunque la elección de su director por parte del Gobierno ha sido también objeto de crítica, lo cierto es que desde su puesta en funcionamiento ha demostrado un ejercicio equidistante e independiente, los grandes escándalos han despaparecido y el panorama se encuentra razonablemente controlado. Con todo, los peligros y los abusos no han desaparecido, cualquiera puede encontrarse con publicidad personalizada que desvela un buen conocimiento de nuestro nivel socio-económico por parte de la empresa, incluso se pueden dar casos como el de una niña a cuyo nombre se envió publicidad sobre alimentos infantiles y una felicitación por su primer cumpleaños, sin saber que había fallecido a la semana de su nacimiento. También es cierto que este fallo espeluznante sucedió antes de establecerse las garantías legales y que las propias empresas del sector, a través de la Asociación de Marketing Directo, han creado la lista Robinson para excluir de la publicidad de las empresas que componen dicha asociación, a aquellas personas que no deseen recibir información comercial, para lo que basta con comunicar la voluntad de ser incluido en la lista.

Como ya se ha comentado, los ficheros de titularidad privada están en buena medida controlados y no presentan grandes peligros para la intimidad, más allá de la invasión publicitaria que también se produce por medios como el buzoneo, menos selectivos pero igual de eficaces. Un buen ejemplo de su control es que todos los ficheros con datos personales han de ser inscritos en la APD para que conozca su composición, estructura, procedencia de la información, etc. En los

seis primeros meses de campaña se registraron más de 200.000 ficheros de empresas privadas, frente a unos 21.000 públicos. La principal diferencia no fue de carácter numérico sino de cumplimiento de la ley, ya que según la memoria de la APD (1994) las Administraciones Públicas incumplieron de forma notoria con la obligación de registrar sus ficheros. Esto hará que en 1995 frente a los 4.765 inscritos por éstas, sólo haya 8.173 privados.

Es asimismo llamativo el número de reclamaciones y denuncias presentadas ante la Agencia, 81 en 1994 y algo más de 300 al año siguiente, cifras absolutamente modestas si se tiene en cuenta el grado de desarrollo que el procesamiento automatizado de datos de carácter personal tiene en España, y el elevado número de ficheros inscritos. En cuanto a las preocupaciones evidenciadas por las denuncias y reclamaciones, el comportamiento es similar al de otros países con mayor tradición, casi el 60 % se refieren a ficheros relacionados con la solvencia patrimonial, el crédito y la morosidad; sin embargo resulta igualmente llamativo el desinterés por datos de gran impacto sobre la intimidad, como son los relacionados con la salud y los procesados por las fuerzas y cuerpos de seguridad del Estado. No es extraño si se tienen en cuenta las dificultades de acceso en dichos casos.

La preocupación ciudadana por los ficheros de solvencia y morosidad es simple expresión de las repercusiones que pueden tener los datos erróneos, sobre todo si se deniega el derecho de información, acceso, rectificación y cancelación, uno de los aspectos más denunciados ante la Agencia. Asimismo era práctica abusiva de las entidades de crédito el manipular datos relativos a la salud de los clientes, en consecuencia *sensibles*, porque ellas mismas realizaban los seguros de vida necesarios para obtener un crédito. Todo esto llevó a la APD a elaborar sendas instrucciones, la una relativa a los servicios de información sobre solvencia patrimonial y crédito, en la que se establecen los criterios de calidad de los datos y la notificación al afectado; la otra, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.

Así como las denuncias y reclamaciones han sido hasta ahora exiguas, también son pocos los expedientes sancionadores abiertos. Los procedimientos se han concentrado en tres sectores de actividad: el marketing directo, la información sobre solvencia y cumplimiento de obligaciones dinerarias, y el sector financiero. El caso más frecuente es el del tratamiento de datos personales sin consentimiento del afectado y, en el caso de las actividades relacionadas con el marketing directo, destaca por su frecuencia la utilización de datos procedentes del padrón municipal y el censo electoral, las principales fuentes ilícitas de datos personales para uso comercial. Esto ha desembocado en multas de hasta 50

millones de pesetas y a casos tan llamativos como el de RENFE, que utilizó los datos de filiación sindical de sus empleados para descontar de las nóminas tras una huelga convocada por CCOO y CGT; la Agencia consideró muy grave utilizar datos de los empleados sin su permiso, más aún si se trata de información sensible como la ideología política o sindical, dándose la circunstancia de que se produjeron además 6.139 errores en la aplicación del descuento (el 75 % de los afiliados a los sindicatos convocantes).

Excepción hecha de las sanciones administrativas de la APD, hasta hace poco las violaciones más graves de la privacidad, como pudo ser el caso de Publicest u otros, quedaban en esencia impunes, por cuanto la manipulación informática de datos personales *sensibles* no estaba tipificada como delito. Sin embargo el Código Penal de 1995 en su título X (delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio), contiene una serie de artículos (197 a 201) en los que se regula el denominado delito informático. Además prevee una agravación de las penas, entre otros: en los casos de actos que afecten a datos de carácter personal *que revelen la ideología, religión, creencias, salud, origen racial o vida sexual*; cuando la víctima sea un menor de edad o un incapaz, y cuando *los hechos se realicen con fines lucrativos.*

La situación en el sector público es más preocupante, porque la ley es menos estricta que con el privado en lo relativo al ejercicio de los derechos del ciudadano; además, las bases de datos públicas son las que contienen mayor cantidad y variedad de datos *sensibles*. Sin embargo esto no podrá seguir así mucho tiempo, como quiera que no estamos solos sino en un contexto europeo, nuestra legislación debe ser adaptada a la comunitaria, pues es la que uniformiza el espacio común. En este sentido se aprobó en julio de 1995 una directiva sobre datos personales con el objeto de homogeneizar la legislación de los miembros de la Unión, que forzará a reformar las leyes españolas, ya que la misma no distingue los ficheros públicos de los privados, incluye entre los datos personales que deben ser protegidos el sonido y la imagen propia, aludiendo expresamente a la vigilancia por videocámara; regula los ficheros manuales, además de los automatizados, siempre que se trate de un archivo estructurado, asimismo incluye la afiliación sindical entre los datos personales de especial protección, y detalla de forma muy precisa las excepciones a la prohibición general de recabar y almacenar datos sensibles, cosa que no hace la legislación española.

Uno de los primeros ámbitos que se han visto afectados es el policial, objeto de preocupación de los socios comunitarios, ya que condensa cantidad de información altamente sensible, cuya inexactitud o mal uso pueden producir consecuencias funestas sobre los afectados. Incluso en nuestro país va creciendo la expectación ciudadana, ya se ha visto que en 1994 sólo unas pocas reclamaciones y denuncias ante la Agencia de Protección de Datos - el 4%- se refe-

rían a los ficheros policiales, sin embargo al año siguiente ya eran el doble (8%). Además de ser un comportamiento similar al de otros países, el procedimiento vigente concede una discrecionalidad excesiva a la administración para acceder o no a informar al interesado, lo que desanima a la mayoría, a pesar de que tanto el Cuerpo Nacional de Policía como la Guardia Civil disponen al menos de 58 ficheros de investigación policial, en los que con mayor o menor detalle constamos todos los españoles mayores de catorce años, algunos menores y bastantes extranjeros.

Es tal la importancia que reviste esta información, su exactitud y adecuado tratamiento, que en el convenio por el que en 1995 se creó la Oficina Europea de Policía, más conocida como *Europol*, se puso especial énfasis en la protección de los ciudadanos frente a los datos y su manejo. Entre otras medidas de garantía se establece una autoridad común de control, independiente, compuesta por representantes de todos los países miembros, para garantizar que el almacenamiento, el tratamiento y la utilización de los datos no vulneren los derechos de las personas. Además, el convenio regula el derecho de acceso a la información por parte de los ciudadanos afectados, así como la obligatoriedad de verificar y actualizar todos los datos almacenados en un plazo máximo de tres años.

Aparte de este sistema existe otro relacionado con el Tratado de Schengen, firmado por varios países, entre ellos España, para la libre circulación de ciudadanos, que contempla el intercambio de información entre las respectivas policías mediante un banco de datos común con información relativa a casi un millón de personas, y para acceder al mismo es imprescindible poseer una legislación interna que proteja la intimidad de los ciudadanos. La negativa de la Guardia Civil a publicar la estructura de sus ficheros sobre terrorismo, tal como obliga la LORTAD, dio lugar a un pulso con la Agencia de Protección de Datos, quien señalaba que además de incumplirse la ley, esta actitud afectaría a la colaboración antiterrorista con los miembros del grupo. A pesar de esto el Consejo de Ministros del 16 de febrero de 1996 acordaba declarar secreta *la estructura, organización, medios y técnicas operativas de las Fuerzas de Seguridad del Estado en la lucha antiterrorista; así como sus fuentes y cuantas informaciones o datos puedan revelarlas.* Con esta decisión los servicios de información de la policía y Guardia Civil recibían el mismo tratamiento que el CESID obtuviera en 1986 y que ha servido al Gobierno para denegar los polémicos documentos a los tribunales. Además de controvertido por dudosamente legal, este acuerdo significaba de hecho la imposible cooperación policial con el grupo de Schengen, por todo lo cual el director de la APD decidió abrir expediente sancionador contra la Benemérita. Aunque al mes siguiente la secretaria de Estado de Interior ordenó legalizar los ficheros, las cosas continuaron así hasta que a finales del mes de septiembre el Gobierno decidió rectificar, obligando al insti-

tuto armado a legalizar su situación y a que permitiera que la APD inspeccione sus archivos informáticos sobre terrorismo.

Podríamos continuar analizando otros muchos casos como puede ser el de las policías locales, que por su dispersión quizá sean más difíciles de controlar, la de Hacienda, cuyo ordenador llamado *Rita* maneja datos *sensibles* de millones de españoles, la Seguridad Social, y tantos otros organismos oficiales; sin embargo parece más interesante contemplar otros aspectos igualmente importantes como la seguridad y la transparencia.

Al decir seguridad no nos referimos a los problemas que plantea la transmisión de datos o la protección de los sistemas frente a intromisiones, sino al cuidado que ponen las Administraciones Públicas en la custodia de los datos personales. El escándalo de 1992 es bastante revelador en este sentido, pero sin llegar al robo existen otras formas de negligencia. La elaboración del último padrón de habitantes, por ejemplo, se ha contratado en algunos municipios importantes con la división informática del primer grupo español de grandes almacenes; se puede alegar que con otros servicios como la recaudación, la limpieza viaria, la recogida de basuras, la grúa, etc. se hace lo mismo. La diferencia radica en que para elaborar el padrón municipal de habitantes se recaba gran variedad de datos, algunos de los cuales y todos en conjunto, caen dentro de los denominados *datos sensibles.* No se trata de prejuzgar a la empresa concesionaria, ni de valorar las posibles medidas de seguridad contempladas en los contratos, no parece muy diligente que una empresa privada con tantos intereses en el sector comercial, y en consecuencia ávida de datos, sea la encargada de recopilar y procesar los relativos a unos ciudadanos que actúan en la creencia de que sólo su administración va a tener conocimiento de los mismos. En fín, una cosa es ser consciente de que la seguridad absoluta es imposible, pero otra es tentar con insistencia a la suerte.

Resulta paradójico que cuando se trata de denegar al ciudadano el ejercicio de sus derechos, y aun a la propia justicia, la administración invoque el interés general y la seguridad del Estado como razones inapelables, y sin embargo se muestre tan amnésica en otras ocasiones. Así, en el año 95 el censo electoral se vendía en el mercado negro por siete millones de pesetas. El origen es muy simple, los partidos y sucedáneos que se presentan a las elecciones, por ejemplo 1.034 en las últimas municipales. Como quiera que el censo electoral se reparte entre los partidos que presentan candidaturas, y parte son fingidas para obtener estos datos, que después son vendidos principalmente a empresas de marketing directo. Para la APD es muy difícil controlar el movimiento de datos si se mantiene este descontrol con el censo, por lo que ha propuesto que se entregue a los partidos uno especial en el que sólo figuren los datos de carácer público (nombre, apellidos y dirección), como se estila en otros países para proteger con más

eficacia los datos sensibles. Además sugiere que se introduzcan señas, como errores ortográficos deliberados, para poder detectar el origen ilegal. Algo parecido permitió a la Agencia multar a varias empresas con hasta quince millones de pesetas por utilizar el censo como fuente fraudulenta. Todo sucedió a raíz de la denuncia de un ciudadano que recibió publicidad a su nombre con un error en su segundo apellido, el mismo con el que figuraba en el censo electoral.

4. A modo de conclusión

Despues de todo lo visto parece claro que es imposible alcanzar la protección absoluta en cuanto al tratamiento automatizado de datos de carácter personal, el marco legislativo y los organismos específicos no son garantías suficientes. La experiencia nos demuestra, además, que los delitos cometidos en el entorno tecnológico, por su naturaleza extraordinariamente dinámica, aún están poco contemplados en la legislación penal, por lo que en ocasiones quedan impunes. Sea como sea, parte de la responsabilidad está en nuestra mano. Como indicó Simon Davis, director general de Privacy International:

> "hay que aprender a decir no. No a las empresas, no a las instituciones públicas que nos piden datos personales para introducirlos en sus bases informáticas y que tratan de asignarnos un número de control. Si no paramos la invasión informática, dentro de diez o veinte años el futuro será del Gran Hermano."

Sin pretensiones catastrofistas, podemos afirmar que el papel de las tecnologías de la información al servicio de la vigilancia puede sumirnos en el *síndrome del pez rojo*, esto es, la sensación de estar en una pequeña pecera, atentamente observados por la maquinaria estatal. Además de nuestra presencia en cientos de sistemas informáticos que poseen todo tipo de datos, aún los más sensibles, un hipotético Gran Hermano podría controlar nuestros movimientos, ideas, gustos y tendencias al milímetro. Gracias a las tarjetas de crédito, además de comprar sin correr riesgos de llevar el dinero encima, es posible conocer casi todo de nosostros, a dónde vamos de vacaciones, cuánto gastamos y cómo, si leemos o no y qué tipo de literatura, y hasta nuestra vida sexual, pues aunque en el extracto bancario figure marisquería, por los números se sabe si es una casa de citas. ¿Se habían dado cuenta de que cuando se detiene a un terrorista, la policía se incauta de todo menos tarjetas de crédito? Es lógico que si no han de quedar rastros, mucho menos se pueden dejar huellas electrónicas, tan indelebles y fáciles de seguir. ¿Qué pasaría si los denominados monederos electrónicos terminan por desplazar al dinero convencional en nuestra vida diaria? ¿Y si las Administraciones públicas entrecruzaran todos sus ficheros? ¿Y si llegaran a unir las bases de datos públicas y privadas en manos de alguien, por ejemplo el Estado? ¿Y si todo adquiriera escala mundial? La respuesta es simple, nos situaría en una tesitura de indefensión prácticamente absoluta.

Como ya se ha señalado no pretendo pintar una escena claustrofóbica, si la ley ha respondido hasta ahora mal que bien tutelando los derechos de los ciudadanos, nada nos hace pensar que las cosas vayan a empeorar en el futuro. Es posible que la domesticación tecnológica produzca un efecto democratizador, por cuanto ya no será necesario la intermediación de magistratura alguna para que los ciudadanos accedan a los sistemas donde consten datos relativos a su persona. Poseyendo las mismas tecnologías y vías de comunicación, no es muy descabellado pensar que cada cual pueda ejercer directamente los derechos de acceso, control, puesta al día, rectificación, etc. de sus datos personales. Sea como sea parece claro el irresistible ascenso de las tecnologías de la información y sus efectos esencialmente positivos, asimismo bien podemos imaginar que en tanto se universalice el acceso a las mismas, deberán redefinirse los términos relacionales, hasta alcanzar algo así como un pacto informático entre los individuos y las organizaciones que establezca las reglas de un juego en el que el ciudadano quede a salvo de la pecera.

5. Bibliografía

Para la redacción de este articulo se han utilizado las memorias del Defensor del Pueblo y las de la Agencia de Protección de Datos, así como la prensa diaria entre los años 1991 y 1996.