LA INCIDENCIA DE LA SOCIEDAD DE LA INFORMACIÓN O SOCIEDAD DE LA VIGILANCIA EN LOS DERECHOS FUNDAMENTALES: UNA TRANSFORMACIÓN DE SU RÉGIMEN DE EJERCICIO Y PROTECCIÓN.

Ana Aba Catoira

1. INTRODUCCIÓN

Una comprensión adecuada del significado y alcance de los derechos fundamentales exige caracterizarlos como categorías "radicalmente históricas", utilizando una expresión acuñada por el Profesor PÉREZ LUÑO. Esta historicidad de los derechos se pone de manifiesto no sólo en su reconocimiento inicial, tras luchas constantes de los individuos contra el poder establecido, sino también en su contenido variable, pues, como bien señala FIORAVANTI "cada tiempo histórico produce su propia cultura de los derechos privilegiando un aspecto respecto a otro o poniendo las libertades en su conjunto más o menos en el centro del interés general" (*Los Derechos Fundamentales*, Trotta, Madrid, 1996, pág.24).

Retomando las palabras de HÄBERLE "los derechos fundamentales son la respuesta, según la experiencia histórica a las principales amenazas para el hombre (derechos humanos) y para el ciudadano (derechos civiles) en el Estado constitucional, puesto que las específicas situaciones de peligro cambian históricamente y nuevos instrumentos para combatirlos deben desarrollarse" (*La libertà fondamentali nello Stato costituzionale,* La Nuova Italia Scientifica, Roma, 1993, pág.177).

Y es que con el desarrollo de las sociedades aparecen nuevos movimientos reivindicativos que introducen novedades en el ámbito de los derechos fundamentales como derechos constitucionalmente reconocidos y garantizados. Estos nuevos derechos son la respuesta del Derecho a las nuevas necesidades históricas que, en ocasiones, no conducen al reconocimiento de nuevos derechos o libertades sino a una adaptación o redefinición de derechos ya conocidos. En el ámbito del derecho a la intimidad sucede esto último, pues los avances de la sociedad sobre todo en lo referente a las nuevas tecnologías, obligan a redefinir el contenido clásico de la intimidad como derecho a proteger en la Sociedad de la Vigilancia multidireccional.

Pues bien, el desarrollo tecnológico como acontecimiento histórico reseñable, en cuanto que está causando una auténtica revolución a todos los niveles, pone de manifiesto esta variabilidad de los derechos, en concreto del derecho a la intimidad. Dice el Profesor PÉREZ LUÑO que la actualidad del derecho a la intimidad podemos medirla con un método que califica como "dramático", ya que consiste en "comprobar la frecuencia e intensidad con la que cada derecho es violado" ("Dilemas actuales de la protección de la intimidad" en *Problemas actuales de los Derechos Fundamentales*,

Universidad Carlos III de Madrid, BOE, Madrid, 1994, pág.311). Así, de su contenido dinámico y de su concepto histórico y cultural, dependerá la determinación del espacio que comprende la intimidad protegida, pues según el Tribunal Constitucional "Son realidades intangibles cuya extensión viene determinada en cada sociedad y en cada momento histórico y cuyo núcleo esencial en sociedades pluralistas ideológicamente heterogéneas deben determinar los órganos del poder judicial" (STC 171/1990, 5 de noviembre, FJ 4º).

2. LA SOCIEDAD DE LA VIGILANCIA: LA INFORMACIÓN COMO INSTRUMENTO DE PODER

Estamos metidos de lleno en un auténtico proceso revolucionario equiparable o superior a otros que ya ha vivido la Humanidad. Este cambio brutal, este ir hacia delante sin marcha atrás, se produce en el ámbito de las nuevas tecnologías, no ya en el campo más elemental de la informática sino en el más avanzado de las telecomunicaciones o, aún más, en la aplicación de las telecomunicaciones a la informática y a la radiodifusión, esto es, la telemática, la telefonía o la televisión digital. Así pues, el avance imparable e incluso temible de las nuevas tecnologías, permite obtener, procesar y almacenar datos de manera ilimitada, con lo que desaparecen las fronteras espaciales y temporales y se produce una importante novedad que estamos empezando a vivir, la instauración de un nuevo modelo de sociedad conocido como "Sociedad de la Información", con una nueva configuración de las relaciones sociales y económicas que suponen la transformación del Poder y del Mercado, donde la información se erige como uno de sus valores y, quizás, el bien más preciado. Esta realidad va a suponer un ataque a los derechos que protegen la vida privada de las personas, ya que "una vez convertida la información en protagonista del nuevo sector cuaternario, ahora añadido a los tres sectores económicos tradicionales, se ha desatado la fiebre de acopio de datos. Las sociedades y empresas de hoy miden su dinamismo y empuje por la cantidad y calidad de sus informaciones. La trascendencia económica de la información ha generado un apetito insaciable de obtenerla por cualquier medio y a cualquier precio y es directamente responsable de determinadas prácticas abusivas que hoy, por desgracia, acechan el libre ejercicio de la privacidad en nuestra vida cotidiana" (PÉREZ LUÑO, A.E.: "Dilemas ... cit., pág.321).

Las nuevas técnicas en materia de telecomunicaciones nos sitúan ante dos elementos esenciales: 1. Los nuevos medios como instrumentos de control y vigilancia; y, 2. Los derechos fundamentales que resultan más afectados por el avance tecnológico, que va a suponer una profunda transformación de su régimen de ejercicio y una insuficiencia de las técnicas tradicionales de protección. Nos referimos a derechos como la libertad de expresión, la libertad de información, los derechos de la personalidad encabezados por el derecho a la intimidad, la inviolabilidad de las comunicaciones y algunos más.

La situación en la que nos encontramos se podría sintetizar del siguiente modo: la inexistencia de fronteras tanto espaciales como temporales posibilita la libre circulación de datos, por lo que la apropiación o captación de datos transformables en información y su transmisión otorgan poder, entendido en su acepción más amplia. La informatización de la sociedad, principalmente a través de la conexión y entrada en Internet, hacen posible que los ciudadanos estén cada vez más próximos a la economía, a la cultura o al ocio, lo que posibilita un nivel de vida más alto o si se prefiere una más alta calidad de vida, por lo que, el acceso a las telecomunicaciones es una ventaja para los ciudadanos que podrán disfrutar de sus notables beneficios.

En este sentido, el acceso a la información "ilimitada" es bueno y es positivo porque nos enriquece, pero esto se ha de valorar sin olvidar dos elementos importantes que veremos después y que ya apuntamos. El primero, que el acceso a la información no es universal, pues, cuando menos, unos tendrán más fácil el acceso que otros, con lo que aparece una estructuración de la sociedad, quizás aún no en nuevas clases sociales, pero si en grupos que tienen acceso a la información y grupos que no lo tienen. Y, en segundo lugar, que la Sociedad de la Información aporta indudables ventajas a través de las nuevas tecnologías, pero nos somete a un riesgo continuo y grave de estar permanentemente controlados o vigilados no ya por un par de ojos –Gran Hermano estatal- sino por millones de ellos, y más aún, se trata de un riesgo que, en la inmensa mayoría de los casos, ni lo conocemos o somos incapaces de valorar. En cualquier caso, es necesaria la generalización del acceso a las tecnologías o nuevos medios de información porque las tecnologías no son sólo una amenaza para los derechos fundamentales sino un nuevo medio de hacerlos efectivos.

Dicho esto, cabe plantearse si los ciudadanos conocen las amenazas que para su privacidad suponen las nuevas tecnologías de la comunicación, a lo que podríamos contestar que en el noventa por ciento de los casos, no, pues, ante este nuevo mundo apasionante sólo vemos las ventajas que reporta una libre y voluntaria, pero, también, continua, cesión de datos. Y ocurre que las innumerables ventajas que nos proporciona la revolución tecnológica no nos dejan ver los nuevos problemas que se generan en la sociedad y que hasta el momento eran desconocidos y para los que, a día de hoy, el Derecho aún no tiene todas las soluciones.

Y es aquí, llegados a este punto, cuando hemos de preguntarnos por el Estado, cuestionando su papel en su función de proteger a sus ciudadanos, qué mecanismos se han establecido para facilitar el acceso universal a la información, en cuanto derecho fundamental. Pues, si todos los ciudadanos llegan a participar, mínimamente por igual, de las ventajas y oportunidades que suponen las nuevas tecnologías, estaremos avanzando en desarrollo y calidad de vida. Si, por el contrario, no todos quedamos integrados, estaremos creando una sociedad con notables desequilibrios y diferencias de clase, propiciados por el acceso o por la falta de acceso a la información. Pensemos, por ejemplo, en las ventajas que la telemedicina aporta a los habitantes de las áreas rurales que podrían ver mejorada sensiblemente su asistencia sanitaria; en el teletrabajo que introduce una flexibilidad del horario y aumenta el acceso de las mujeres al mercado laboral; o en la teleeducación que lleva la enseñanza universitaria a cualquier punto remoto del planeta.

Lo anterior nos permite avanzar la existencia de importantes problemas sociales que plantea la nueva Sociedad de la Información, en cuanto que concede maravillosas oportunidades a aquéllos que tienen fácil el acceso –medios económicos- y que la Información, la lucha por conquistarla, se constituye en motor que propulsará una revolución social que supondrá el paso del mundo real a un mundo virtual. Pues, a nadie se le escapa, y de hecho existe coincidencia en la opinión pública, que las nuevas tecnologías acentúan los desequilibrios y las desigualdades y es que, de hecho, de que le sirve Internet a las capas sociales que no tengan cubiertas sus necesidades básicas. Francamente, sólo plantear la cuestión suena a absurdo.

Así pues, podrán participar en la Sociedad de la Información aquéllos que tengan, precisamente eso, Información, en cuanto conocimiento o formación para poder acceder a ella, lo que en el mundo de las telecomunicaciones se resume en acceso a un ordenador y, evidentemente, saber utilizarlo. La cultura, la enseñanza o el saber son bienes que han de facilitar los poderes públicos y de ahí la necesidad de un compromiso del Estado para con sus ciudadanos que no se extingue tras el período de escolarización sino que exige una formación continuada, una puesta a punto, pues, el avance incesante de las tecnologías así lo exige. En definitiva, se trata de que el Estado asuma el compromiso de crear una Sociedad de la Información para todos, en la que todos quedemos

perfectamente integrados, y esto encuentra su fundamento constitucional en el artículo 9.2º de la Constitución donde se establece que "corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social". Este compromiso que han de asumir los Estados, obliga a facilitar el acceso a las tecnologías sobre las que se construye el nuevo modelo de sociedad, pero también les obliga a proteger a sus ciudadanos y, más concretamente, la efectividad de sus derechos fundamentales, ante los peligros que de ella derivan.

Dicho esto, pasaremos a ver el fenómeno de la Sociedad de la Información desde el otro lado, desde la posición del vigilante, del observador y captor de datos.

Siempre se ha ejercido un control sobre los ciudadanos para satisfacer el ansia de conocimiento del Estado, la Iglesia o incluso de los demás particulares. En un principio, la mayor información estaba en manos de la Iglesia (ojos de Dios) que controlaba todo lo que acontecía en las vidas de sus fieles, mientras que, posteriormente, el Estado fue ocupando esta privilegiada posición en cuanto que necesita, cada vez más, tener datos sobre sus ciudadanos para gestionar su actividad pública, ya sea sobre censos, materia tributaria o servicios concretos como la sanidad, seguridad o educación. Ahora bien, este nuevo modelo de Sociedad actual ha transformado las relaciones sociales, pero también las de carácter económico y laboral, por lo que debido a la redistribución del Poder, que obedece a una descentralización y disgregación multidireccional hacia todos los centros de obtención de información, la recopilación de datos no está únicamente en manos del Estado. Las nuevas tecnologías van desplazando al gran poder público que de forma inexorable va cediendo terreno a los poderosos sujetos privados que han hecho de la obtención y tratamiento de la información un moderno instrumento de control social, por lo que la noticia, el conocimiento, los datos, etc, han dirigido o encauzado los procesos de obtención de poder. Llegado a este punto de la exposición, resulta conveniente precisar que por Poder entendemos influencia sobre los individuos y los grupos sociales en que se integran, que hace posible mover la voluntad de las personas sin recurrir al uso de la fuerza o de la coacción, ya hablemos de poder político, de poder económico o de poder social.

Así, fueron los estados quienes primero desarrollaron técnicas de investigación, de obtención de datos, de recogida de información, con el ansia de que la información les diera poder. El conocimiento se adquiere a través de las técnicas de espionaje o de vigilancia secreta que suministran información reservada y, también, gracias a la investigación científica que proporciona otro tipo de conocimiento, sinónimo de desarrollo y progreso, y que, a diferencia, del primer tipo de conocimiento no se mantiene en secreto sino que se divulga para dar el poder intelectual del saber científico o académico a la sociedad. Sin embargo, ahora, en la conquista de la información, se enfrentan empresas y estados o si se prefiere, poderes privados y poder público, para controlar y abarcar el mayor número posible de datos sobre los ciudadanos, lo que va a suponer una invasión de la privacidad, ya que, si bien gracias al progreso el Estado puede controlar más intensamente la vida de sus ciudadanos, también podrán hacerlo los poderes privados que persiguen la información para sus fines propios de carácter eminentemente económico. Este peligro que para los derechos fundamentales de los ciudadanos supone el conocimiento ilimitado de datos personales, su cesión y tratamiento informatizado, fue previsto por la Constitución española de 1978, que en el párrafo 4º de su artículo 18 estableció que "una 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". Es ésta, sin duda, una previsión constitucional que, a día de hoy, ya se ha quedado corta ante el ascenso imparable de la telemática.

Por tanto, sucede que, frente al peligro principal del que se avisaba en el Estado de la Vigilancia que surge tras la Segunda Guerra Mundial, en cuanto posibles agresio-

nes provocadas por las técnicas estatales de vigilancia, en las sociedades de la Vigilancia el problema gira en torno al uso que se le da a la información obtenida. Y así, se comprobará, después, como la concepción clásica de la intimidad que la concibe de forma estática en cuanto "pretensión, libertad, poder e inmunidad a disponer de un ámbito de vida personal sustraído a cualquier tipo de intromisión perturbadora o, simplemente, no deseadas" da paso a una concepción de la intimidad abierta y dinámica como "posibilidad de conocer, acceder y controlar las informaciones que conciernen a cada persona" (PÉREZ LUÑO, A.E.: "Dilemas ...", cit., pág.315). De este modo, se produce un desplazamiento del peligro generado a través de la obtención de la información al uso o destino de la misma. En otras palabras, se sabe que ahí está el vigilante (múltiple), de hecho casi nunca se capta la información de forma oculta porque el observador permanece visible y nos pregunta y nos solicita abiertamente información personal y la obtiene cedida voluntariamente por el ciudadano, pero, sucede que no se conoce el destino último de los datos cedidos. Así, el enorme valor económico que la información personal o reservada alcanza en el mercado, despierta un enorme interés que se dirige hacia su obtención, aunque sea invadiendo el ámbito privado de las personas. En este sentido, en la Sociedad de la Vigilancia, la protección de los derechos de los ciudadanos reside, no en la evitación de la obtención de datos, sino, en que los titulares de esos datos tengan la posibilidad real de controlar el destino y uso de los mismos, pudiendo incluso prohibir su difusión, de ahí la necesidad de los mecanismos legales de protección.

Por tanto, aún cuando la vigilancia sigue siendo el gran mecanismo de obtención de poder, ha ido evolucionando haciéndose más tolerable para los ciudadanos que, en no pocas ocasiones, ceden sus datos voluntariamente a cambio de una compensación, pero con un evidente desconocimiento de las desventajas o perjuicios que tal cesión acabará ocasionándoles. La información obtenida se almacena en bases de datos en manos del gobierno o de las empresas privadas, con fines institucionales o comerciales específicos, pues los datos que se recogen y archivan corresponden a cuestiones o preguntas concretas y determinadas. Y es que las bases de datos (recopilación, almacenamiento y recuperación automatizadas) rara vez contienen información obtenida de forma encubierta, si bien el uso que posteriormente se le dará, es decir, el objetivo al que se destina, no es abiertamente conocido por la ciudadanía.

Bentham ideó un panóptico como ilusión de una vigilancia permanente que hacía creer a los prisioneros que estaban bajo un control constante, y que es posible trasladar a la idea que sustenta estas páginas. Cierto es que los ciudadanos no somos los prisioneros que alumbraron el panóptico benthiano, pero si que el poder del estado funciona automáticamente sobre los ciudadanos sin necesidad de coerciones, pues los vigilados por el ojo público no tienen otra opción más que la de someterse a la vigilancia estatal ejercitada de forma continuada. Así, la vida del país discurre bajo la atenta mirada vigilante del Gran Hermano que controla el cumplimiento de las obligaciones tributarias de los ciudadanos para el sostenimiento de la Hacienda Pública, el censo para la elaboración de las listas electorales, la productividad de los trabajadores públicos, las cualidades morales y personales de sus ciudadanos a través de la elaboración de estadísticas que proporcionan los perfiles de la sociedad, etc. La información se obtiene sin necesidad de acudir a coerciones, de forma voluntaria, respondiendo al esquema del panóptico participativo, pues aquellos que no cumplan la obligación de proporcionar los datos requeridos por el Estado se autoexcluyen de la estructura social.

Algunos ejemplos del control estatal sobre los datos personales de los ciudadanos son los siguientes:

La identificación de los ciudadanos a través de la especificación de la raza, sexo, edad, situación familiar y laboral, que se realiza a través de la expedición del Documento Nacional de Identidad y del Número de Identificación Fiscal, que constitu-

yen, sin duda, dos fuentes de obtención de datos personales, cuyo uso entraña graves peligros para el derecho a la intimidad y a la vida privada de los ciudadanos. En el supuesto de que un ciudadano se niegue a identificarse en cumplimiento de un requerimiento policial, la ley prevé una medida que busca obtener la información personal que se niega a dar y que justifica la limitación de los derechos del afectado.

En cuanto a la elaboración del censo electoral, hay que decir que, a pesar del carácter voluntario del voto, es decir, del ejercicio del derecho de sufragio activo, la ley (art.32 LOREG) impone la obligación de la inscripción censal.

Además, la Administración económica y tributaria puede controlar la situación económica individual y familiar de sus ciudadanos para un correcto ejercicio de los derechos y deberes fiscales. El Tribunal Constitucional ha reiterado que "la Administración está habilitada, también desde el plano constitucional (art.31.1° C.E.), para exigir determinados datos relativos a la situación económica de los contribuyentes", "para evitar una distribución injusta de la carga fiscal" se justifica la necesidad de "una actividad inspectora especialmente vigilante y eficaz, aunque pueda resultar a veces incómoda y molesta" (STC 110/84, 26 de noviembre, FJ 3°; 76/90, 26 de abril, FJ 9°).

La Administración sanitaria recopila cantidad de datos muy privados sobre los que recae un deber de confidencialidad que busca mantener en secreto toda la información relativa a las estancias o procesos en hospitales o centros sanitarios, asi como un deber de secreto de los facultativos sobre su actividad médica. Los datos de esta naturaleza resultan especialmente sensibles al conocimiento de terceros públicos o privados, por lo que sobre ellos recae una obligación especial de protección.

La Videovigilancia (LOVI) se concibe como medida de prevención de actos delictivos, protección de personas y conservación y custodia de bienes, y supone un instrumento eficaz para el cumplimiento de la misión que el artículo 104.1° de la Constitución atribuye a las Fuerzas y Cuerpos de Seguridad del Estado que han de contar con medios adecuados y suficientes para ello. Así pues, aun cuando la grabación de imágenes y sonidos con videocámaras en lugares públicos y su posterior tratamiento, suponen una intromisión en la intimidad de las personas, no constituye una actuación ilegítima por ser una medida que busca asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de los espacios públicos, así como la prevención de delitos y faltas. Además, la Ley Orgánica de Videocámaras especifica las garantías que, en el debido respeto de los derechos y libertades de los ciudadanos, se han de respetar en todas las fases de autorización, grabación y uso de las imágenes y sonidos obtenidos.

Las bases de datos, archivos y registros, recopilan información personal de los ciudadanos, con lo que entramos de lleno en la relación tensa entre la libertad de información y el derecho a la intimidad, pues la vida privada constituye un evidente límite que restringe el acceso a la información en estos soportes contenida (art.105.b C.E.).

En otro ámbito de la Administración tenemos a los medios de comunicación social, teniendo presente el Estatuto de RadioTelevisión Española que en su art.4.d) habla de cómo el principio de respeto al honor, fama, vida privada de las personas y los derechos y libertades que reconoce la Constitución, han de inspirar la actividad de los medios.

Y podemos seguir hablando de mecanismos de vigilancia pública a través de los que el Estado obtiene cuantiosa y valiosa información personal, como son las Comisiones de Investigación o, en otro ámbito radicalmente diferente, los análisis de sangre en las pruebas de alcoholemia (art.380 CP) o en la investigación de paternidad (STC 7/94, 17 de enero, FFJJ 2° y 3°).

Esta afirmación se refuerza aún más en los sectores privados, pues los ciudadanos tienen más interés en participar en ellos ante las innumerables ventajas que se les

ofrecen a cambio de su participación que se traduce en cesión de datos personales. La información al ser consensual se convierte en producto comercial con un importante equivalente económico, a diferencia de la que obtienen los gobiernos a través de los servicios de inteligencia o en cumplimiento de las obligaciones legales de sus ciudadanos, por lo que aquéllos que la obtienen hacen de ella un instrumento de obtención de poder. No obstante, tanto unos como otros, es decir, la información que conforma los informes públicos y privados, contienen datos de carácter personal de los ciudadanos sometidos a una intensa vigilancia multidireccional.

Los datos que en un inicio se obtienen cedidos por los titulares para un uso específico y conocido, son tratados en las bases de datos como mercancía, alcanzando un valor muy alto en el mercado de la información. Una vez que dicha información es interpretada por las máquinas y conectada a la Red, entra en la rueda de la información que empieza a girar y a girar convirtiendo a aquellos datos iniciales que identifican a un ciudadano o a un consumidor, dependiendo de la mirada que lo vigile, en una bola gigantesca e imparable de información.

En cuanto a la obtención de datos hemos recalcado el carácter voluntario típico de las cesiones, con la intención de obtener una participación beneficiosa en el mercado de la información, como son productos varios, descuentos y, como no, información continuada a la que queremos acceder. Evidentemente, cuando entramos en una página de Internet lo hacemos en nuestro interés de conocer más y siendo conscientes de la amenaza de observadores que no han sido invitados a conocer nuestros datos personales. Sin embargo, no rehusamos a beneficiarnos de las nuevas tecnologías a pesar del precio que hay que pagar. Y así se recopila y almacena información de carácter personal para abrirse a continuación el proceso de su comercialización. Los datos de naturaleza diversa que se obtienen a través de diversas fuentes se comparan, se relacionan y amplían, y así por ejemplo una compañía de seguros puede buscar coincidencias con los archivos médicos para decidir sobre los seguros a negociar, lo que conduce a la inclusión o exclusión de los ciudadanos de una cartera de clientes potenciales. Por ello, aun cuando el poder está disperso, y las bases de datos son muchas y diversas, al entrar en relación por intereses comerciales comunes se van a cruzar datos y el "vigilante" se hace más poderoso y temible obteniendo una mayor y completa información.

La ampliación de datos conlleva la transparencia absoluta de la vida de los ciudadanos: cuantos son en casa, cual es la renta familiar, si viven de alquiler o en una vivienda de su propiedad, si tienen coche y la clase de seguro, donde van de vacaciones, que les gusta comer, cual es el presupuesto para manutención, ropa, ocio ... En definitiva, a través de las nuevas técnicas de información y del tratamiento ilimitado de datos, nos convertimos en hombre y mujeres visibles hasta la transparencia, sujetos a una constante vigilancia que se ejerce desde muy distintas direcciones, por lo que aquéllo que quizás se le escape a un par de ojos, otro par lo capta.

Día a día, las bases de datos de carácter privado se van haciendo con el control de la mercancía, desplazando a las bases estatales menos poderosas, y esto no sólo por su número y dimensiones, sino también y sobre todo por su influencia sobre los ciudadanos que ceden más alegremente información propia. La vigilancia que se realiza con ojos privados resulta más fructífera que la vigilancia estatal por aquel carácter voluntario de la cesión de datos, pues el ciudadano entiende que se beneficia con la participación recíproca en el mercado de la información sin pensar en las desventajas o inconvenientes indirectos que derivan del intenso control. Pensemos en las técnicas de vigilancia que operan sobre nosotros y con las que colaboramos a cambio de los servicios o utilidades que nos reportan. Las tarjetas de crédito, los cajeros automáticos, las tarjetas de salud inteligentes, etiquetas electrónicas, la vigilancia videográfica, bolsas de empleo en páginas de Internet o el abono a los canales digitales. Mención aparte merece Internet, sin duda convertida en

el gigante de la Vigilancia que abastece de información a todos los poderes de este nuevo modelo de sociedad. Los ordenadores y la telemática han reestructurado los modos de producción y el sector servicios, habiendo menos trabajadores, más flexibilidad laboral, más consumo y más marketing dirigido a éste. El acceso diario a Internet a través de las páginas web o la utilización constante del correo electrónico, permiten obtener datos personales de todos aquellos que se conectan sin reparar en el alto precio que se ha de pagar por utilizar estos medios tecnológicos, cada vez que se enciende el ordenador personal. Y es que, si uno lo piensa detenidamente, está claro que son muchas las ventajas, pues quién va a renunciar a tener toda la información que precisa casi de forma instantánea a su producción en cualquier lugar del mundo, o a trabajar de forma más rápida y completa o a enviar su correspondencia o curriculum vitae vía Internet. Se nos facilita el trabajo, se nos proporciona toda la información sin límites y todo ello contribuye a mejorar nuestra calidad de vida. Los innumerables beneficios que nos proporciona la Sociedad de la Información no son gratis, y el usuario, el individuo que sólo ve ventajas en las telecomunicaciones, cede gustoso datos personales que al fin y al cabo circulan por la Red de forma imperceptible. No obstante, no hay que olvidar que el mercado selecciona a sus clientes, quienes van a disfrutar de sus productos o sus servicios, por lo que la mirada panóptica observa con mejores ojos a los que tienen más ingresos, una vida estable y discreta o aquéllos que más les interesan porque darán mayores beneficios. Así, aun cuando la vigilancia actual se construye sobre una participación recíproca y consensual que beneficia a ambas partes, no será equitativa, pues será más y mejor para unos que para otros.

Una de las ventajas que para los ciudadanos supone el avance de las técnicas de vigilancia y el acceso a tanta información, es que ahora no sólo quedan sometidos a control los individuos. Se ha producido un aumento de la vigilancia jerárquica, de arriba abajo, pero también a la inversa, al quedar el poder controlado por los ciudadanos. Un ejemplo claro de contravigilancia lo encontramos en las técnicas de vigilancia y control que facilitan el trabajo de las Fuerzas de Seguridad en la lucha por la seguridad ciudadana, pues si las terminales de ordenador conectadas a los coches patrulla permiten obtener, simplemente por introducir los datos de una matrícula, información personal sobre un investigado, posibilitan, también, un seguimiento de la cantidad y calidad del trabajo de los agentes. La contravigilancia permite un control mutuo pudiendo la opinión pública seguir la actividad de los órganos de poder que ya no siempre serán vigilantes sino también vigilados. Esta vigilancia multidireccional alcanzó un punto álgido, en cuanto escándalo internacional, en el llamado caso Lewinsky donde nos encontramos con que la utilización de técnicas de vigilancia o espionaje como las escuchas y grabaciones telefónicas destaparon un escándalo que salpicó, y de que manera, al Presidente de los Estados Unidos, cuya vida amorosa saltó a todos los medios de comunicación, amén de los problemas de política interna, pudiendo ser seguida por todos los ciudadanos.

El surgimiento de la contravigilancia responde a la preocupación por controlar la vigilancia radical a la que se encuentran sometidos los ciudadanos necesitados de técnicas de protección de su privacidad. La necesidad de contar con barreras de carácter legal y de carácter ético o moral, como los códigos deontológicos, comisiones y códigos voluntarios en el sector privado, dispositivos legales para bloquear o controlar el trasiego de información personal, exige un compromiso de los poderes públicos, pero también de los privados que han de actuar con autocontrol. Ahora bien, esto pone de manifiesto a su vez cierta contradicción, pues por un lado la ciudadanía demanda mayor libertad de información, pero, también, respeto de los derechos de la personalidad; por un lado, se pide seguridad, pero con reducción de los niveles de vigilancia.

Georges Orwell en *1984*, creó el Gran Hermano como un monstruo que siempre nos vigila convirtiéndose en un gran tirano político. Ante el enorme giro que ha dado la situación, cabe preguntarse quien es el monstruo que nos vigila una vez entrado el siglo XXI y metidos de lleno en la era de las super tecnologías. Indudablemente el temor se

proyecta sobre un nuevo tirano del que no hay escapatoria y que se llama vigilancia multidireccional ejercida desde los sectores privados. Rusell Baker en 1998 en las páginas del New York Times escribía "[...] la vigilancia no se limita a las autoridades oficiales como el FBI, el fiscal Kenneth Starr o el policía local con su pistola radar. Hubo una vez un ciudadano privado que, con su cámara de videoaficionado, filmó a la policía de Los Ángeles 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 [...]".

3. LA INCIDENCIA EN LOS DERECHOS FUNDAMENTALES

La aparición de las nuevas tecnologías ha supuesto una profunda transformación de la sociedad y con ella muchos aspectos del régimen jurídico de los derechos fundamentales, tanto en lo que concierne a su ejercicio como a sus garantías o protección. En este sentido, si hablamos de Sociedad de la Información, los derechos más afectados serán aquéllos cuyo contenido y forma de ejercicio tienen relación directa con el proceso de comunicación, por lo que nos referimos a las libertades del artículo 20 de la Constitución y a los derechos que, tradicionalmente, entran con ellas en colisión. Es decir, los derechos de la personalidad íntimamente ligados a la intimidad de las personas y garantizados en el artículo 18.1º de la Constitución, aunque quizás sea más exacto hablar de privacidad o vida privada, sin olvidar otros bienes constitucionales como la protección de la juventud y de la infancia, tal como establece el párrafo 4º del citado artículo 20. En cualquier caso, la afectación o transformación que se produce en el régimen de estos derechos y libertades, obedece al auge de la información tanto en su vertiente de emisión o difusión como en la de recepción.

La incidencia de las nuevas tecnologías es diferente según los derechos afectados. Para las libertades de expresión e información han supuesto un campo ilimitado para su ejercicio y expansión al no existir fronteras espaciales ni temporales haciendo que el proceso de transmisión sea continuo e ilimitado y resultando más difícil controlar lo que se difunde, asi como quien lo hace, por lo que los límites jurídicos tradicionales resultan inoperantes, como es el caso del secuestro judicial como garantía de los derechos. Por tanto, esta posibilidad de transmitir y recibir información continua tiene también su cara negativa que incide sobre los derechos que, tradicionalmente, resultan lesionados por dicho ejercicio ilimitado. De acuerdo con el artículo 20.4º de la Constitución, los derechos del Título I con mención expresa del honor, la intimidad y la propia imagen (art.18.1º); la protección de la juventud y de la infancia o protección de la moral sexual de los jóvenes (habrá de tenerse especial cuidado con la publicidad y exhibición de artículos pornográficos, asi como con los contenidos de la programación) limitan el ejercicio de dichas libertades. De este modo, a mayor libertad de información (garantía del pluralismo democrático) mayor afectación de la vida privada, porque se multiplican de forma indefinida los centros de obtención y tratamiento automatizado de datos, desde donde se exprime al máximo a las personas en su afán por obtener mayor cantidad de información.

3.1º- Incidencias en el esquema tradicional de las libertades de expresión e información: art.20.1º.a) y 20.1º.d) C.E.

Los ciudadanos tienen el derecho fundamental de acceder a la información veraz como un instrumento esencial de conocimiento de los asuntos que cobran importancia en la vida colectiva y que, por lo mismo, condiciona la participación de todos en el buen funcionamiento del sistema de relaciones democráticas auspiciado por la Constitución,

asi como el ejercicio efectivo de otros derechos y libertades (STC 220/91, 25 de noviembre, FJ 4°). En todo caso, el acceso a la información ha de estar asegurado para todos y que la información sea veraz y nunca transmitida en régimen de monopolio garantizando la pluralidad y libertad sobre las que se asienta el principio democrático.

Las citadas limitaciones a la libre información han de ser aplicadas tras realizarse una ponderación en la que cobra peso específico la posición preferente del derecho a la información en cuanto garantía institucional de la opinión pública fundamento del pluralismo democrático. Así, la libertad de comunicar información veraz alcanza su máxima eficacia frente al derecho al honor o a la intimidad que se debilitan como límites (STC 336/93, 15 de noviembre, FJ 4°) cuando es ejercida por los profesionales de la comunicación a través de los "cauces normales" de formación de la opinión pública, cabe preguntarse entonces cuál es el lugar que ocupan en este ámbito las nuevas tecnologías de la Sociedad de la Información.

El derecho a la libre información requiere la intervención del Estado, se necesitan medios para poder ejercer el derecho y, por tanto, que existan accesos adecuados. En este sentido, la radiotelevisión ha sido configurada como un servicio público presidido por el pluralismo, esencial al principio democrático, y cuya concesión para ser gestionada por una empresa privada queda condicionada a la disponibilidad de un recurso limitado de dominio público como son las ondas radioeléctricas, si bien la escasez del bien ha sido salvada por la televisión por cable primero y ahora por la televisión digital. Junto al criterio de la escasez que fundamenta la necesaria igualdad de acceso a las ondas, se han aplicado otros. Siendo la televisión el medio más utilizado, tiene una mayor penetración social, lo que conlleva la necesidad de un mayor control de sus contenidos y de si efectivamente se respeta el pluralismo, todo lo que conduce a un fuerte control o regulación desde el poder público. Dentro de la esfera privada y, por tanto, fuera del servicio público, quedan los operadores de televisión por satélite y televisión digital, suponiendo ésta última un aumento considerable del número de canales, una selección del producto a través del pago por visión, un control del usuario y consumidor por la conexión a los canales temáticos, y, en definitiva, a través de los servicios que proporciona este medio televisivo, un estudio y vigilancia del ciudadano.

Las nuevas tecnologías introducen cambios cuantitativos y cualitativos respecto a los medios de comunicación tradicionales: aparecen nuevos medios como el correo electrónico, los chats y los foros de discusión; surge un importante número de empresas dedicadas a servir productos de información, por lo que hablamos de las implicaciones económicas de las nuevas tecnologías en el mercado audiovisual; y, por derivación, se produce una acumulación de poder que influye en la opinión pública poniendo en peligro el requisito constitucional del pluralismo, en tanto que la concentración de medios tanto escritos como audiovisuales restringen la oferta plural, ya que aun cuando aumentan los cauces de emisión y recepción de información, la fuente o el origen confluye en el mismo o mismos. El pluralismo se convierte en un objetivo a conseguir dentro del medio, pues, desde fuera, la oferta si mantiene al menos apariencia de pluralidad a través de la diversidad de medios. Así pues, la concentración de poder en pocas manos, uno de los males de la Sociedad de la Información, conduce a la instauración de imperios multimedia en cuyo seno se produce la información, se distribuye y comercializa y se crean los medios tecnológicos necesarios para su comunicación (por ejemplo los descodificadores).

La digitalización –conversión de la información o datos en números- e Internet posibilitan que la información que posee el centro emisor pueda desconcentrarse a través de la selección que lleva a cabo el consumidor, seleccionando de la oferta de información aquélla que es de su interés. Asimismo, Internet supone la desaparición de la distinción entre medios de comunicación públicos y privados al estar la comunica-

ción totalmente abierta en cualquier dirección porque cualquiera puede difundir o transmitir información, con lo que el proceso deja de ser bidireccional para convertirse en un proceso multidireccional, además de que confluyen todos los medios de comunicación, telefónica (correo), escrita (boletines, foros de discusión) y audiovisual.

Así pues, sucede que en los nuevos procesos de comunicación, las dos partes actúan como emisores y receptores de información participando activamente en la formación de la opinión pública con lo que se maximaliza la libertad de expresión, si bien en el ejercicio de la libre información resultan afectados elementos como la veracidad, se flexibilizan los derechos del artículo 18 de la Constitución como límites a su ejercicio, y la máxima protección que la Constitución depara a la información producida por los cauces ordinarios y a través de los profesionales, se pone cuando menos en entredicho cuando se realiza a través de Internet. Por tanto, estos parámetros no resultan trasladables al mundo Internet, lo que obliga a su redefinición.

3.2º. El derecho a la intimidad y el desarrollo del art.18.4º C.E.: El derecho a la autodeterminación informativa.

El enorme crecimiento del valor de los datos personales en la Sociedad de la Información abre nuevas vías de peligro para los derechos de las personas en lo referente a la protección de su intimidad y vida privada. En otras palabras, para que no se produzca una intromisión continua en la vida privada se ha de potenciar una política y medidas adecuadas para su aplicación, tendente a controlar al máximo los datos que circulan en el Mercado de la Información. Esto es, los aspectos relativos a su contenido, exactitud, quienes tienen acceso a ellos y su utilización y uso, son cuestiones, entre otras muchas, que están encima de la mesa, en cuanto que preocupan a la sociedad y sobre las que se ha de trabajar en busca de respuestas adecuadas y efectivas en materia de política informática o de las telecomunicaciones. Así pues, el Estado está obligado a actuar para dar cobertura jurídica a las demandas legítimas de sus ciudadanos y, en este sentido, ha de asumir "una posición beligerante en la defensa de los derechos de la persona, no puede permanecer ajeno a esta tensión dialéctica entre consumo de información y defensa de la personalidad. Ambos términos del binomio son irreductibles: la libertad de información, de la que es exponente típico la libertad informática, se nos ofrece como un componente necesario de una sociedad libre, pluralista e igualitaria. Por otra parte, sin embargo, la defensa del ciudadano y de su esfera de intimidad personal y familiar constituye un criterio de legitimación política para toda sociedad democrática" (ÁLVAREZ-CIENFUEGOS SUÁREZ, J.Mª: *La defensa de la intimidad de los ciudadanos y la tecnología informática,* Aranzadi, Madrid, 1999, pág.14).

El avance tecnológico y el desarrollo científico son imprescindibles para la sociedad que pide de forma constante información, pero en esa misma sociedad se ha despertado una conciencia hacia una demanda de mayor protección de la intimidad y de la vida privada sometidas a constantes peligros derivados del acceso a la información personal como bien de consumo tanto desde el Estado como de los poderes privados, sin olvidar, por supuesto, a los propios ciudadanos como consumidores de información. La conclusión no puede ser otra que la necesidad de encontrar un equilibrio entre libertad de información y derechos de la personalidad, en la búsqueda de la protección de los datos personales que afectan a la intimidad y vida privada de las personas. Como bien se dice en el Informe Nora-Minc "la información y la participación progresan juntas" y sólo "un poder que disponga de las informaciones apropiadas podrá favorecer el desarrollo y garantizar la independencia del país: él es el mediador de los apremios vitales" (Cita tomada de A.E. PÉREZ LUÑO: *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 1991, pág.364).

En páginas anteriores, se ha puesto de manifiesto como los derechos, por ser categorías históricas, evolucionan con las sociedades en las que se gestan, se maduran y se hacen realidad. Con el derecho a la intimidad sucede esto mismo que se confirma tanto en su regulación como en su régimen de protección y tutela, en cuanto van a resultar insuficientes los esquemas jurídicos tradicionales para frenar las nuevas amenazas surgidas con el desarrollo de las tecnologías.

Tradicionalmente, la intimidad quedaba a salvo si el individuo titular del derecho seguía unas mínimas pautas de prevención frente a intromisiones o conocimientos ajenos de las facetas o esferas más íntimas o privadas de su vida personal y familiar. En la actualidad, la prevención resulta a todas luces insuficiente cuando un cuchicheo puede ser desvelado por mecanismos de alta precisión tecnológica. Nadie está a salvo de la vigilancia ni siquiera dentro de las cuatro paredes de su domicilio porque el desarrollo de la técnica provee al mercado de un sinfín de instrumentos de vigilancia para la captación y reproducción de imágenes, sonidos, etc, que se traducen en datos y, posteriormente, en información o conocimiento sobre la persona, sin que aquél que ha sido observado y vigilado llegue a tener constancia de ello. Ante tal panorama, la posibilidad de defensa o de tutela de los derechos de la personalidad, íntimamente ligados a la dignidad de la persona y a una mínima calidad de vida, disminuye de manera inversamente proporcional al desarrollo de las tecnologías.

En ningún caso, se puede configurar la intimidad como una libertad tradicional para cuya tutela resulta suficiente la abstención del Estado o la mera protección en cuanto control para que no se produzcan intervenciones ilegítimas, pues, ahora, tras la implantación de las nuevas tecnologías, se concibe como un derecho que demanda una tutela que exige una actuación pública que ponga los medios necesarios, a disposición de los afectados, para que éstos puedan controlar el uso que se hace de sus datos personales. En definitiva, pues, hay que resaltar la insuficiencia en una sociedad desarrollada de la configuración del derecho a la intimidad como un derecho de defensa frente a intromisiones indebidas por no autorizadas o consentidas, y hay que poner de manifiesto la necesidad de entenderla como un derecho positivo de control sobre las informaciones que afecten a cada sujeto.

El derecho a la intimidad, como bien es sabido, se reconoce en el artículo 18.1° de la Constitución y en el párrafo 4° del mismo artículo como derecho frente a las nuevas tecnologías. Esto sin olvidar que aparece expresamente mencionado como límite al ejercicio de las libertades de expresión en el artículo 20.4° y, más adelante, en el artículo 105.b, en el ámbito de las relaciones entre los ciudadanos y la Administración Pública en materia de acceso a archivos y registros administrativos. Así pues, en la Constitución, la intimidad recoge el concepto de derecho de defensa o garantía de no intromisión, reafirmado en su configuración como límite a las libertades del artículo 20, con lo cual este derecho no permite a terceros, ya sean públicos o privados, disponer sobre el espacio de intimidad personal o familiar que queda reservado o sustraído a intromisiones no consentidas.

La importancia y significado del derecho a la intimidad queda patente no sólo por su reconocimiento constitucional como derecho fundamental ligado a la dignidad de la persona, sino, también, por su caracterización, en cuanto derecho de la personalidad, en la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, intimidad y propia imagen, como derecho irrenunciable, inalienable e imprescriptible. Un carácter que recoge el Tribunal Constitucional en STC 21/1992, 14 de febrero, FJ 3°, al conectar los demás derechos con la intimidad, a la que califica como bien sin el cual no es realizable no concebible siquiera la existencia en dignidad que a todos quiere asegurar la norma fundamental.

Delimitar el derecho que se reconoce en el párrafo 1° del artículo 18 de la Norma Constitucional supone hablar de "el atributo más importante de la intimidad como

núcleo de la personalidad, es la facultad de exclusión de los demás, de abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimiento intrusiva como a la divulgación ilegítima de esos datos" (STC 142/1993, 23 de abril, FJ 7º).

El consentimiento o la voluntad resultan fundamentales para delimitar que es lo íntimo o privado para cada persona y así "quien por su propia voluntad da a conocer a la luz pública unos determinados hechos concernientes a su vida familiar, los excluye de la esfera de su intimidad" (STC 197/1991, 27 de octubre, FJ 4º).

El derecho a la intimidad se configura como derecho de libertad frente a potenciales agresiones a nuestra dignidad y libertad, por lo que, según establece la Constitución en su previsión del 18.4º, se reconoce el derecho a estar informado sobre los datos almacenados que nos afectan, su contenido y la finalidad específica de los respectivos ficheros. Hablamos, sin duda, de un derecho de libertad como derecho de autodeterminación informativa para poder controlar nuestros datos y que supone para el Estado un doble deber, por un lado negativo, en cuanto no revelación de datos o información personal sin el consentimiento expreso del titular, y, un deber positivo, en cuanto facilitación del derecho de acceso a los ficheros para los afectados (STC 254/93, 20 de julio, FJ 6º). Se requiere el consentimiento del afectado para la utilización de datos personales, siempre con una finalidad legítima. El derecho de libertad informática o informativa es el derecho a controlar el uso de los datos introducidos en un programa informático (habeas data) y permite al ciudadano expresar su oposición a que sus datos sean utilizados para fines distintos de aquel legítimo que justificó su obtención (STC 11/1998, 13 de enero, FJ 4º).

En cuanto al término que se ha de utilizar ante la nueva configuración del derecho a la intimidad, se discute si mantener este mismo o, por el contrario, es conveniente manejar una expresión proveniente del ámbito anglosajón privacy en cuanto vida privada o privacidad. Resulta evidente que cuando se habla de intimidad se hace referencia a un ámbito más estricto que cuando hablamos de vida privada o de nuestra privacidad, por lo que, aunque la esencia de ambos conceptos es la misma, tienen un alcance distinto porque lo privado engloba a lo íntimo pero lo supera. En este sentido, la jurisprudencia del Tribunal Europeo de Derechos Humanos viene diferenciando ambos conceptos por razón de amplitud, al entender que la privacidad no debe reducirse a un círculo íntimo donde cada uno pueda llevar su vida conforme a sus propias pautas sin sujeción a cánones sociales (STEDH *Costello-Roberts*, 25 de marzo de 1993, A 247-C). El concepto cada vez más manejado de privacidad viene importado del *common law* y, como sucede con todo, tiene partidarios y detractores. En el grupo de estos últimos podemos señalar a MARTINEZ DE PISÓN quien cuestiona la utilización de categorías propias de otros ámbitos jurídicos aun cuando afirma la incuestionable influencia de este concepto en la configuración actual del derecho a la intimidad (*El derecho a la intimidad en la jurisprudencia constitucional*, Cívitas, Madrid, 1993, pp.26-27).

La cuestión es si la protección de los datos personales en cuanto derecho de control sobre los mismos entra dentro del ámbito del derecho a la intimidad en sentido estricto. Y, ciertamente, el nuevo derecho de autodeterminación informativa, surgido de la evolución del derecho fundamental del artículo 18.1º protege la vida privada de las personas que puede ser revelada a través de la obtención de los datos personales porque las informaciones de esta naturaleza versan sobre multitud de aspectos o facetas de la existencia de los individuos que un significado restringido propio de la intimidad no los cubre y protege. La jurisprudencia constitucional española recurre a la intimidad para preservar las manifestaciones más reservadas de la vida personal y familiar; el cuerpo (STC 37/1988, 15 de febrero, FJ 7º); relaciones paterno-filiales porque considera que la filiación forma parte del ámbito propio y reservado de lo íntimo, es un derecho que se extiende a los aspectos de la propia vida y a otros de la vida de otras personas con las

que se tenga una vinculación familiar estrecha (STC 231/1988, 2 de diciembre, FJ 4º; 197/1991, 17 de octubre, FJ 3º): la muerte (STC 231/1988, 2 de diciembre, FJ 8º). En otras ocasiones recurre al concepto de privacidad entendiendo que "la protección constitucional del domicilio es una protección de carácter instrumental , que defiende los ámbitos en que se desarrolla la vida privada de la persona [...] Por ello, a través de este derecho no sólo es objeto de protección el espacio físico en sí mismo considerado, sino lo que en él hay de emanación de la persona y de la esfera privada de ella.

Los datos personales afectan a todas las facetas o aspectos de la vida personal, familiar, laboral, profesional, sanitaria, económica, lúdica ..., por lo que parece más apropiado hablar de un derecho de control sobre los datos relativos a la persona (STC 254/1993, 20 de julio, FJ 7º) y lo que es relativo a una persona es privado mientras el interesado no lo haga público. Se trata de un derecho que nace de la previsión del artículo 18.4º como garantía de la intimidad, pero con suficiente entidad para hablar de él de forma autónoma como libertad informática o autodeterminación informativa que nace de la pretensión de tutela frente a los peligros derivados de las tecnologías, pues la recopilación de datos y su tratamiento automatizado conduce a la reivindicación de la privacidad, como tutela de todos los derechos de la personalidad: relaciones familiares, sociales, sexuales, comunicaciones, domicilio, operaciones económicas ...

La evolución del derecho a la intimidad ha desembocado en una nueva configuración que le da un significado estricto o un significado más amplio, tal como se comprueba en la jurisprudencia constitucional, pero que se reconduce al reconocimiento de una ámbito protegido y reservado frente a la acción y conocimiento de los demás, necesario según las pautas de nuestra cultura para mantener una calidad mínima de vida humana" (STC 207/1996, 16 de diciembre). La informática y las nuevas tecnologías posibilitan el conocimiento de datos personales que corresponden a la esfera íntima y personal (intimidad en sentido estricto), pero que pueden salir de ella porque aún siendo de carácter personal –privados- y, por consiguiente, su titular quiere mantenerlos excluídos del conocimiento ajeno, no pertenecen a lo más íntimo de esa esfera. En este sentido, para garantizar esa reserva de lo privado, de lo propio y personal, se establece una garantía constitucional consistente en otorgar al afectado el derecho de controlar sus datos personales o, más concretamente, la utilización, uso o destino de sus datos una vez almacenados. Lo que se produce desde la Constitución es una extensión del alcance del derecho a la intimidad para otorgar tutela frente a nuevos peligros que surgen en las sociedades tecnológicamente desarrolladas, y este derecho para ser efectivo necesita de nuevas formas o técnicas de protección mucho más complejas que las tradicionales de abstención de intervención y, en su caso, instrumentos jurídicos de reparación del daño causado. Ahora se prohíben conductas que supongan intromisiones ilegítimas en la esfera privada de la persona y que de producirse se sancionarán, pero, también se ha de asegurar el control sobre los datos para evitar usos indebidos de la información de carácter personal, si bien "el nivel de autodeterminación, es decir, de disposición de uno mismo sobre sus propios datos, dependerá de la naturaleza de éstos y de su mayor o menor proximidad al núcleo de la intimidad. No obstante, aunque, cuando nos encontremos fuera de él, no será posible impedir que circule información sobre nuestras personas, siempre hemos de estar en condiciones de asegurarnos de su calidad y de conocer y controlar su utilización" (P. LUCAS MURILLO DE LA CUEVA: *El derecho a la intimidad*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 1993, pág.57).

Así pues, el desarrollo del mandato constitucional contenido en el artículo 18.4º, nos introduce de lleno en el estudio del derecho a la autodeterminación informativa o derecho a controlar los datos e informaciones que afecten a la privacidad de las personas, y que nos obliga a analizar cual es la respuesta legislativa en el marco de la Sociedad tecnológica.

4. PROTECCIÓN DE DATOS PERSONALES

El desarrollo de las nuevas tecnologías en el ámbito de la obtención de datos ha sido tratado en Europa con preocupación evidente. La conversión de la información en conocimiento sobre los ciudadanos y sus datos personales es una notoria característica de la Sociedad de la Información, que se construye sobre la ingente cantidad de información que se obtiene a un mínimo coste, la velocidad con que se capta y se transmite, y que ha de contar con instrumentos de protección de los titulares de los datos, que se establecerán atendiendo a una clasificación de la información. Es decir, de acuerdo con el valor que ésta tenga, así será el grado de protección que se le dispense en la legislación específica. Así pues, lógicamente, quedarán más protegidas aquellas informaciones o datos de carácter personal cuyo conocimiento afecta al derecho a la intimidad, como derecho a evitar el conocimiento de datos, su almacenamiento y tratamiento, que han de quedar controlados facilitando el acceso del titular afectado.

Las primeras respuestas legislativas giran en torno a la creación de garantías para los derechos fundamentales más amenazados por la Sociedad de la Información, que en el caso español suponen un desarrollo de la previsión constitucional contenida en el artículo 18.4º como limitación del uso de la informática. La insuficiencia del texto español queda de manifiesto si se compara con el artículo 35 de la Constitución portuguesa de 1976, donde se hace una completa regulación de la utilización de la informática. En Portugal se reconoce el derecho de todos los ciudadanos de acceder a las informaciones contenidas en registros que les afecten, conocer el uso al que se destinan, pudiendo exigir su rectificación y puesta al día. A continuación se declara que la informática no debe servir para procesar datos relativos a las convicciones políticas, a las creencias religiosas o a la vida privada de las personas, salvo lo que se refiera al tratamiento, con fines estadísticos, de datos no identificables. Se prohíbe atribuir a los ciudadanos un número nacional único.

El constituyente portugués reflejó en un precepto constitucional los problemas que surgen en la sociedad de la información en cuanto afectación de los derechos de las personas por la utilización de nuevas tecnologías y, evidentemente, contrasta con la previsión del constituyente español. Así las cosas, le corresponde al legislador constituído, llamado expresamente desde la Constitución, desarrollar una política legislativa de protección de datos personales y, consiguientemente, limitar no sólo el uso de la informática sino el de todas las tecnologías. Poco a poco, el legislador va tomando conciencia de los adelantos e innovaciones tecnológicas, que demuestran la insuficiencia de la limitación del uso de la informática en orden a la protección de los derechos de las personas afectadas, por lo que las nuevas respuestas y desarrollos legislativos han de adecuarse a la realidad tecnológica que supone una continua amenaza y agresión para la vida privada de las personas. Nos encontramos pues, que ante la imposibilidad de controlar los centros de obtención de datos provocada por la vigilancia multidireccional, hay que hacer un esfuerzo por proteger los datos en su almacenamiento y tratamiento, con especial interés por aquéllos calificados como más sensibles. Estamos ante la reivindicación y efectiva protección de un derecho de autodeterminación informativa o de libertad informática, ejercitable por los titulares de los datos personales.

Así las cosas, decíamos que en Europa estos temas han sido una evidente preocupación y encontramos a nivel supranacional una mayor regulación de la intimidad informática que en cada uno de los estados individualmente considerados.

Las primeras decisiones al respecto son la Resolución de la Asamblea General de la ONU, de 19 de diciembre de 1968, "Derechos del hombre y progreso de la ciencia y de la técnica"; un Estudio encargado por la UNESCO a la Comisión Internacional de juristas sobre el derecho de protección a la vida privada en 1972; un Informe del

Secretario General a la Comisión de Derechos Humanos de 1974 sobre "Aplicaciones de la electrónica que pueden afectar a los derechos de las personas y límites que se deberían fijar para estas aplicaciones en una sociedad democrática".

El punto de inflexión lo marca el Convenio Europeo aprobado el 28 de enero de 1981 y elaborado por el Consejo de Europa que recoge unos principios considerados básicos para la protección de datos y crea, además, un Comité Consultivo con la función de formular propuestas para mejorar su aplicación. Los principios finalista (pertinencia de los datos, utilización no abusiva y derecho de olvido); principio de lealtad; principio de exactitud; principio de publicidad; acceso individual y principio de seguridad, se recogen en el Capítulo II del este texto europeo. Posteriormente, los Acuerdos *Schengen* de 14 de junio de 1985 buscaron la coordinación entre estados para llevar a cabo la aplicación de los principios contenidos en el Convenio.

El Informe Bangemann "Europa y la Sociedad global de la Información", recomendación del Grupo con dicho nombre hecha al Consejo Europeo el 26 de mayo d 1994, va a precisar cuales son las directrices o líneas a seguir por los estados miembros de la Unión para lograr la protección de los derechos y de la vida privada de sus ciudadanos ante el avance de las nuevas tecnologías.

En este orden de cosas, el Informe considera imprescindible para alcanzar una plena Sociedad de la Información varias cosas: conseguir una actuación conjunta de todos los estados miembros y una implicación de los agentes públicos y privados, asi como de toda la ciudadanía. Asimismo, evitar la creación de una sociedad de dos capas en la que sólo una parte de la población tenga acceso a las tecnologías y a los beneficios que éstas reportan. Se hace necesario fomentar las competencias de las fuerzas del mercado y poner fin a los monopolios de los operadores de las telecomunicaciones y de los titulares de los medios, para lo que hay que crear las infraestructuras necesarias. Y todo ello acompañado de una efectiva protección de la propiedad intelectual y salvaguarda de la intimidad mediante la regulación del tratamiento electrónico de los datos.

Tras haberse fijado en el ámbito europeo unos principios de acción para avanzar en la protección de los derechos frente a las nuevas tecnologías, el legislador español tiene que asumir el reto de desarrollar una política informática que dé respuesta a problemas de máxima actualidad como la protección de datos personales, la regulación de la contratación a través del comercio electrónico, las firmas digitales, la protección de la propiedad intelectual de las obras vertidas en la Red y de otras cuestiones que van surgiendo día a día.

La mayor preocupación del legislador español en materia de protección de datos, en los dos momentos esenciales como son el de su captación primero y el de su tratamiento o procesamiento automatizado después, se dirige al sector público, a pesar de que se constata en la práctica como los mayores peligros que corren nuestros datos vienen del sector privado. Y es que son las bases de datos privadas las que ocupan una posición de privilegio en materia de obtención de información desplazando a aquellas de carácter estatal, pues, obviamente, los sujetos privados con más recursos económicos tienen un mayor y mejor acceso a las altas tecnologías o entran con más fuerza en el mercado de la información. Son éstos, los Pequeños Hermanos del sector privado, los que recogen o captan mayor número de datos, en muchas ocasiones cedidos voluntariamente por unos ciudadanos confiados que sienten mayor recelo hacia el poder público estatal. Sucede que, tal como hemos intentado reflejar en páginas anteriores, el Gran Hermano exige la cesión de datos como una obligación ciudadana, mientras que las empresas obtienen datos que nosotros cedemos porque nos parecen irrelevantes, sin contenido de información personal o neutro, sin saber que esos datos que regalamos pueden convertirse en sustanciosos al ser susceptibles de elaborar una imagen o un perfil detallado sobre una persona (teoría del mosaico). En otras palabras, se trata de que

cedemos informaciones dispersas, irrelevantes por separado, pero que si se reúnen, lo que sucede con su tratamiento automatizado, se revalorizan al aportar un perfil concreto y detallado de una persona sin que ésta lo sospeche. Por consiguiente, "En una sociedad como la que nos está tocando vivir en la que la información es poder y en la que ese poder se hace decisivo cuando convierte informaciones parciales y dispersas en informaciones en masa y organizadas, la reglamentación jurídica de la informática reviste un interés prioritario" (PÉREZ LUÑO, A.E.: *Derechos Humanos* ... cit., pág.347).

El interés del Estado por la protección de los ciudadanos frente al sector privado obedece no sólo a su función de garante de los derechos fundamentales sino también a un interés propio, pues la repercusión de las nuevas tecnologías en la distribución del poder le afecta negativamente. Y es que, la cada vez mayor asunción de poder por el sector privado, que se hace cargo de servicios que tradicionalmente han sido misión del Estado, como la educación, la seguridad, la medicina o la justicia, van reduciendo el ámbito de actuación público y fortaleciendo a un sector que elige a sus clientes proporcionando sus servicios y asistencia a quiénes están en disposición de pagarlos, acrecentándose la separación entre pobres y ricos, como una consecuencia negativa de esta Sociedad de la Información.

En su Preámbulo la Ley Orgánica de Regulación de Tratamiento Automatizado de los Datos de carácter personal (en adelante LORTAD) expone como "el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad a una amenaza potencial antes desconocida [...] 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 éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo".

Así pues, el legislador español se encuentra ante el reto de establecer una nueva frontera de la intimidad, sustituyendo los límites antes definidos por el tiempo y el espacio, protegiéndola frente a la utilización mecanizada, ordenada y discriminada de los datos. La fijación de esta nueva frontera es el objetivo que marca el artículo 18.4º de la Constitución, que reconoce un nuevo derecho de autodeterminación informativa.

En el desarrollo que se acomete del artículo 18.4º y, por tanto, al legislar sobre el control de los ficheros de datos, entendidos como todo proceso informático que se realiza con ellos, se debería haber actuado con más contundencia. Es decir, precisar con más énfasis el objeto de protección que no es otro que la autodeterminación informativa que da el derecho al titular de los datos personales a controlar todas las informaciones que le afecten, y, en este sentido, si lo que se pretende es regular el tratamiento automatizado de los datos para evitar violaciones de los derechos de las personas, no debería contener un sinfín de excepciones para el ejercicio de la libertad informativa (derechos de acceso, rectificación y cancelación) que introducen o abren vías para que la Administración pueda entrar reglamentariamente a controlar el ejercicio del derecho, lo que supone una violación del derecho del artículo 18 de la Constitución, al no respetarse la reserva de ley establecida en el artículo 53.1º del texto constitucional.

En la misma línea de crítica a la Ley de Regulación de Tratamiento Automatizado de los datos de carácter personal, cabe plantear objeciones a la regulación de la Agencia de Protección de Datos. Este ente de Derecho Público se crea con el reconocimiento de su plena independencia respecto de las Administraciones Públicas en

el ejercicio de sus funciones, pero, el Director de la Agencia es nombrado por el propio Gobierno, el Estatuto es aprobado por el Gobierno y el informe o memoria anual que redacta la Agencia se remite al Ministerio de Justicia y no a las Cámaras. Por tanto, dónde queda la proclamada independencia de este ente público cuando su función le lleva a controlar la aplicación de las normas sobre protección de datos.

En su avance legislativo en el terreno de la protección de datos personales el Parlamento europeo y el Consejo de Europa elaboraron la Directiva 95/46/CE que obliga a los estados miembros en su calidad de norma comunitaria. Derivados de la Directiva 95/46 CE se formulan varios principios que han de inspirar la legislación de los estados miembros para protección de datos, tanto cuando se recogen como cuando son tratados.

Respecto al primer momento de obtención del dato:

- principio de justificación legal y social, en cuanto que ha de estar legitimada la obtención del dato.
- principio de licitud y limitación, que supone la utilización de medios lícitos para la obtención de datos, con lo que se obliga a que exista o consentimiento del afectado o una autorización legal
- principio de fidelidad de la información, pues los datos han de ser exactos y completos, por la que existe un derecho de rectificación y actualización y la obligación de los responsables de los ficheros en este sentido
- principio de pertinencia y finalidad, ya que los datos han de ser los adecuados al propósito perseguido.

Cuando los datos se recogen y archivan se abre la fase de su tratamiento automatizado que ha de seguir los siguientes principios:

- principio de confidencialidad en la custodia de los datos recolectados, que vincula a los encargados y responsables de los registros, obligados por el secreto profesional.
- principio de seguridad, los responsables han de adoptar las medidas necesarias que garanticen la seguridad de los ficheros para que no se produzcan pérdidas ni obtenciones ilícitas de la información almacenada
- principio de caducidad, que impone un plazo de tiempo más allá del cual los datos personales han de ser cancelados. Se entiende que el plazo concluye cuando desaparece la finalidad que motivó su archivo.
- principio del consentimiento del afectado (podemos decir que es el principio básico en materia de protección de datos). Es un derecho de información que tiene el titular de los datos para conocer en todo momento lo relativo a su extracción, tratamiento y archivo, y si es un derecho del titular constituirá el correlativo deber de quien quiere obtener los datos.

De la conjunción de estos principios se extrae el principio de autodeterminación informativa que otorga derechos al titular de los datos, emergiendo como principio esencial y troncal la prestación del consentimiento. Así pues, será él quien pueda decidir sobre su cesión, tratamiento y difusión y, en última instancia, sobre su destino. La Directiva 95/46 es muy clara al respecto y marca los principios sobre los que han de instaurarse las medidas de protección de datos que establezcan los estados para proteger a sus ciudadanos en materia de tratamiento de datos personales. Ahora veamos cual es la situación en que se encuentra la legislación española de protección de datos tras haber recibido un aviso en julio de 1999 desde la Comisión Europea para que le comunicasen las medidas adoptadas para la transposición de la Directiva.

La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), es la respuesta del legislador español a la Directiva 95/46 CE, pero habrá que examinar si el nuevo texto legal resulta suficiente ante las actuales amenazas e intromisiones en la privacidad que se producen en la Sociedad de la Información. Además, se ha aprobado el Real Decreto 994/1999, de 11 de junio, que contiene el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

El objeto de la nueva Ley del año 99 es garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades y los derechos de las personas físicas, y especialmente el honor y la intimidad personal y familiar. Los principios de calidad de los datos, exactitud, puesta al día, y cancelación; el derecho de información en la recogida de datos con la novedad de que cuando los datos no hayan sido recabados del interesado, éste deberá ser informado por el responsable del fichero dentro de los tres meses siguientes al momento de su registro (art.5.4º); y como no el del consentimiento del afectado informan el tratamiento de los datos de carácter personal.

A pesar de que se esperaban más cosas de la nueva Ley se dejan sin respuesta preocupaciones en materia de protección de datos, como la intervención frecuente de la Administración, el acceso a los datos por cuenta de terceros, la independencia de la Agencia de Protección de Datos y de su Director o las garantías que se han de prestar para las cesiones de carácter internacional.

Sobre el tratamiento de los datos personales y la protección de la intimidad en el sector de las telecomunicaciones se elaboró la Directiva 97/66/CE que viene a completar lo dispuesto en la Directiva anterior 95/46/CE para dotar de mayor protección y con un carácter más específico a la intimidad y privacidad de las personas usuarias de las telecomunicaciones. Esta Directiva establece el deber del proveedor de servicios de informar a sus abonados del riesgo de violación de la seguridad en la Red; busca garantizar la confidencialidad de las comunicaciones, prohibiendo las escuchas, grabaciones o interceptaciones; prohíbe el almacenamiento de datos personales sobre los usuarios y abonados que se hayan obtenido con motivo de un proceso de comunicación; trata de evitar llamadas automáticas y molestas; y establece el derecho del usuario de ser excluído de listados públicos ...

El objetivo de la Directiva es el de armonizar las disposiciones de los estados miembros para garantizar un nivel de protección de los derechos y libertades equivalente en todos ellos, y, en particular, del derecho a la intimidad en el tratamiento de los datos personales en el sector de las telecomunicaciones, así como en la libre circulación de datos y equipos y servicios de telecomunicaciones dentro de la Comunidad.

Así pues, la seguridad y la confidencialidad de las comunicaciones, son las bases sobre las que debe elaborarse la legislación específica en materia de telecomunicaciones en cada estado miembro. El 24 de octubre de 2000 es la fecha que se fijó para la transposición de la Directiva.

No obstante lo anterior, la Ley española de Telecomunicaciones 11/1998, 24 de abril, establece ya en su artículo 52 la posibilidad de cifrar todo tipo de información transmitida por telecomunicaciones, regulando al cifrado como instrumento de seguridad de las informaciones. En este sentido, el legislador considera necesario facilitar a la Administración central los aparatos decodificadores que empleen para las inspecciones. Asimismo, la Comisión Nacional del Mercado de Valores ha decidido utilizar la telemática para relacionarse con las administraciones, lo que le aporta mayor celeridad en las operaciones, pero sin merma de la seguridad.

El principio esencial y troncal en materia de protección de datos es la prestación del consentimiento del titular y sobre este principio se configura el derecho de autode-

terminación informativa que, sin embargo, es fácil de soslayar con la aplicación de las nuevas tecnologías. La inexistencia de límites, la velocidad de captación y reproducción, la imposibilidad de ubicar en un espacio físico al responsable, etc, son las nuevas coordenadas o parámetros en el mundo virtual. Así, por ejemplo, cuando el tratamiento y difusión de la información son realizados por los medios de comunicación, nos encontramos con que el periodista recopila datos que envía al ordenador del editor y pasan a ser difundidos por la Red, quedando clasificados en archivos electrónicos. Los medios de comunicación tienen, pues, ante si un instrumento para obtener y multiplicar la información, viendo como el tratamiento automatizado agiliza su trabajo carente ahora de cualquier tipo de fronteras. Por tanto, las telecomunicaciones son una gran amenaza difícil de controlar, ya que cualquier entrada en la Red permite la captación de datos personales que no podemos ni autorizar ni rechazar porque la desconocemos. Los cookies son un buen ejemplo de invasión de la vida privada, pues, a través de ellos, somos identificados cada vez que visitamos el mismo web.

En 1999 se aprobó una Recomendación por el Grupo de Trabajo (Grupo Operativo Internet) en la que se intenta convencer a la industria informática para que avance en la protección de la vida privada de las personas, ajustándose a lo que prescribe la normativa sobre protección de datos. Es decir, el usuario de la Red debe conocer en todo momento el riesgo de conocimiento, recopilación y uso posterior que corren sus datos personales para así poder decidir en consecuencia.

Una Recomendación del Comité de Ministros de la Unión de 19 de febrero de 1999 se dirige a los usuarios de la Red en los siguientes términos:

- Internet no es segura, pero hay medios que deben ser utilizados por los usuarios para proteger sus datos, como la codificación para el correo electrónico confidencial o los códigos de acceso al ordenador personal.
- Cada visita a la Red deja huellas electrónicas que se usan para elaborar perfiles personales de los usuarios, si bien hay medios para ser informados de esas huellas, así como para borrarlas. Además todo usuario puede pedir información sobre las políticas de privacidad.
- Existe la posibilidad de acceder anónimamente a la Red, y si por previsión legal esto no resultara posible, cabe la utilización de un seudónimo que nos identifique ante el proveedor de servicio en Internet.
- Se han de facilitar los datos estrictamente necesarios y ninguno más.
- Estar siempre alerta cuando se nos soliciten datos personales, debiendo preguntar por qué se nos piden.
- Preguntar al proveedor de servicio sobre nuestros datos que tiene acumulados para su procesamiento y por su finalidad.
- Se puede controlar la protección de nuestros datos informando a las autoridades competentes del incumplimiento de las normas de protección y seguridad, o ejerciendo las oportunas acciones legales.
- Proceder con cautela en las cesiones de datos a nivel internacional.

La creciente utilización de los documentos electrónicos en el ámbito profesional está planteando nuevos problemas en materia de protección de datos, pues se producen transferencias de dichos datos a nivel internacional, de modo que no siempre se puede garantizar un nivel adecuado de protección en esos terceros países. Existe una propuesta de Directiva del Parlamento Europeo y del Consejo 98/0191 sobre regulación de la firma electrónica, que obedece a la necesidad en el ámbito de la Unión de facilitar las

relaciones económicas, empresariales y laborales, pero se necesita un contexto seguro para trabajar con certidumbre en el marco de los documentos electrónicos.

El objetivo sería el de garantizar la autenticidad e integridad de la firma electrónica, entendiendo por tal aquella firma en forma digital integrada en unos datos, aneja a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple unos requisitos según la Directiva Comunitaria: está vinculada al signatario, permite su identificación y el signatario la tiene bajo su exclusivo control.

La legislación española sobre esta materia recoge los artículos 25 y 26 de la Directiva 95/46/CE y establece, en el Título V de la Ley de 1999, el requisito para que se realice un movimiento internacional de datos, de que el país de destino proporcione un nivel de protección equiparable al que presta esta Ley. No convence, por la escasa seguridad que proporciona, el criterio del "nivel de protección adecuada" que estimará la Agencia de Protección de Datos. Evidentemente, existe falta de uniformidad en la legislación internacional sobre la protección adecuada y, además, se produce una clara tensión entre la demanda de mayor protección para los derechos de privacidad y los intereses económicos, de gran peso, que presiden la contratación a nivel internacional. Así, para que se conceda la autorización necesaria para transferir datos se exigen garantías que han de ser ofrecidas por quien realice la transferencia como responsable del fichero.

5. CONCLUSIONES

En las sociedades actuales absolutamente informatizadas "el poder ya no reposa sobre el ejercicio de la fuerza física, sino sobre el uso de las informaciones que permiten influir y controlar la conducta de los ciudadanos, sin necesidad de recurrir a medios coactivos" (PEREZ LUÑO, A.E.: "Los Derechos Humanos en la sociedad tecnológica", Cuadernos y Debates, Núm.21, CEC, Madrid, 1990, pág.136).

Si el sometimiento del Poder al Derecho es un pilar sobre el que se asienta el Estado democrático, y los derechos necesitan del Estado para que los reconozca en las normas y los garantice, ello conducirá a la exigencia de que el Derecho vigente ofrezca el suficiente nivel de protección a los ciudadanos ante la amenaza que la acumulación de datos supone para sus derechos, ya esté la información en manos públicas, ya en manos privadas. Pensemos en que los instrumentos de protección que articula el Estado se dirigen a preservar a sus ciudadanos frente a invasiones de su privacidad en dos momentos esenciales en la vida del dato; primero cuando se obtiene o capta la información; después, cuando se realiza su tratamiento automatizado. El Estado ha de proteger al ciudadano frente a los vigilantes públicos y privados (más numerosos), cumpliendo su función constitucional de garante de los derechos fundamentales y asumiendo su compromiso de desarrollo en calidad de vida para todos, que, además, de quedar suficientemente protegidos han de contar con posibilidades reales de integrarse en la nueva Sociedad de la Información. El Estado no puede olvidar su carácter de servidor público, que le obliga a facilitar la existencia de sus ciudadanos proporcionándoles los bienes y servicios adecuados en aras de la consecución de la igualdad material o real (art.9.2° C.E.), pues, la disgregación del Poder y la asunción de éste por diversos ámbitos del sector privado, provoca que algunos de ellos, tradicionalmente a cargo del Estado, sean gestionados por empresas privadas que, a través de la información con la que cuentan, seleccionan el mercado favoreciendo a aquellos clientes que están en disposición de pagarlos, con lo que se acrecienta así la separación de la sociedad en capas como una consecuencia negativa de esta Sociedad informatizada.

Ciertamente, no pasa un solo día sin que en los medios se recojan noticias relativas a la transformación de la sociedad, a causa de los avances tecnológicos que posibilitan una mayor recogida de información. Así, algunas de estas últimas noticias nos hacen llegar nuevos instrumentos o técnicas de vigilancia, especialmente la emisión digital de radio y televisión y, desde luego, Internet, que facilita a los internautas la posibilidad de entrar en distintos portales y, evidentemente, seleccionar la información que quieren recibir, lo que obliga a los medios a luchar por modernizarse y especializarse en la difusión de información. Se produce así una mutua selección entre el emisor y el receptor de información.

Asimismo, debe tenerse en cuenta la vigilancia por medio de pulseras telemáticas de aquellos presos que disfrutan de régimen abierto. Esto supone que aquellos reclusos pueden cambiar la cárcel por una libertad vigilada con sistemas de control electrónicos. Estamos, ante un nuevo instrumento de vigilancia telemática que utilizará la Administración. Esta vigilancia electrónica a través de pulseras localizadoras permitirá que los presos no vayan a dormir a la prisión tal como obliga la legislación penitenciaria. El artículo 86.4° de la Ley General Penitenciaria establece que los internos en régimen abierto han de permanecer como mínimo ocho horas diarias en el centro, debiendo pernoctar en el establecimiento salvo cuando voluntariamente se sometan a este tipo de controles. Cuando el preso entra o sale del domicilio la pulsera activará el receptor instalado en el teléfono que emite un informe por fax o por correo electrónico hasta la central de control de Instituciones Penitenciarias.

Además, una tarjeta permitirá conocer la historia clínica desde cualquier parte del mundo. Son tarjetas inteligentes que suponen importantes avances tecnológicos en la Sanidad. Con la tarjeta inteligente, que empezará a funcionar en Galicia en el año 2005, un ciudadano podrá conocer su historial clínico desde cualquier sitio, pues los chips contendrán sus datos que garantizan la confidencialidad y la autenticidad del propietario para que se le permita acceder a toda la información. Al mismo tiempo, se beneficiarán de la telemedicina que trasladará la información de un centro de salud a otro especializado evitando así traslados innecesarios del propio paciente.