

LA PROTECCIÓN DE LA VIDA PRIVADA ANTE LA VIGILANCIA TOTAL

ESPERANZA MOLERO

INTRODUCCIÓN

Desde finales del siglo pasado, concretamente a partir de las dos últimas décadas, vivimos un nuevo modelo social y económico consecuencia de una nueva era en el ámbito de la comunicación e información que se resume en una frase: «*información es poder*». Por tanto, el siglo XXI está marcado por una sociedad y una economía donde el éxito es sinónimo de capacidad de competir en un marco global informacional.

Sucede pues que, en la actualidad, todos y cada uno de los aspectos de nuestra vida están influídos por las tecnologías, tanto en nuestra faceta pública como ciudadanos como en el ámbito privado como individuos, lo que, sin duda, repercute en la ordenación constitucional. Así, nos encontramos con que las nuevas tecnologías de la información y de la comunicación traen consigo profundas e intensas repercusiones y diversas consecuencias que hacen necesario analizar aquellas cuestiones jurídicas que se plantean con la innovación tecnológica y sus aplicaciones, del mismo modo que deben ser analizadas las respuestas legislativas que se van dando a las nuevas situaciones surgidas. Y es que, en todo caso, el Derecho Constitucional no puede permanecer ajeno a este fenómeno revolucionario, pues la nueva Sociedad, conocida como «Sociedad de la Información», mantiene una estrecha relación con esta rama del Derecho, a la que se le plantean nuevos retos y desafíos. Y bien sabemos que si la norma se aparta de la realidad pierde su vigencia.

En primer lugar, porque la revolución tecnológica ha transformado profundamente todas las relaciones sociales y ha hecho tambalear los pilares del mismo Estado tradicional. Además, porque cuestiones y problemas ya clásicos del Derecho Constitucional necesitan reinterpretarse en el nuevo marco social global. Y, en cualquier caso, porque todas y cada una de las cuestiones afectan de manera más o menos directa a los derechos fundamentales, pilar sobre el que se sustenta el sistema constitucional.

Así pues, nuestro interés por realizar un trabajo de estas características nace, obviamente, de la actualidad de los problemas que se suscitan y que impulsan la creación jurídica, legislativa y jurisprudencial que, hasta el momento, no va a la par del desarrollo tecnológico. Baste recordar como ya el constituyente español en el artículo 18.4º de la Constitución pone su atención en la necesidad de limitar el uso de la informática que puede representar una amenaza para los derechos y libertades de las personas cuando se haga un uso excesivo, indebido e incontrolado de las nuevas tecnologías. Esta preocupación no ha tenido respuesta legislativa hasta mucho tiempo después.

Así las cosas, ante la constatación de las innumerables amenazas existentes en la sociedad tecnologizada que afectan directamente a nuestros derechos fundamentales, este trabajo pretender ser una defensa de la vida privada de las personas que ahora, más que nunca, se encuentra amenazada por usos indebidos o abusivos de las nuevas tecnologías capaces de invadir o penetrar en los ámbitos más íntimos de las personas.

I. LA SOCIEDAD DE LA INFORMACIÓN

El concepto de Sociedad de la Información tiene un indiscutible carácter dinámico como proceso de continuos cambios introducidos a través de las nuevas tecnologías. Los cambios que se han producido a través de los procesos de recopilación, tratamiento y aplicación de las informaciones han supuesto que «la era de la llamada sociedad de la información [...] abre el camino de la revolución cultural más grave que ha conocido la humanidad, tendiendo a desaparecer una especie protegida dentro del género humano, que es la del ser rutinario y gris que entra en una monotonía de comportamiento en sus actitudes en la vida y que no estará permitido o no será posible llevar a cabo ante el nuevo modelo

social que se presenta»¹. Y es que la información como base de la estructura económica y de todas las relaciones se ha convertido en el motor de todos los procesos de producción y de relación y, por consiguiente, quien la posea y sepa tratarla será capaz de dirigirlos. Por tanto, es evidente la importancia de las tecnologías y de su aplicación a la obtención y tratamiento de la información, que hace necesario su aprovechamiento en todos los sectores tanto públicos como privados, y que, además, aún introduciendo numerosos riesgos y peligros para los derechos de las personas no puede dejarnos indiferentes. Y esto es así, hasta el punto de considerarse que la diferencia entre detentar tecnología y no disponer de ella sería la misma que la existente entre «la civilización con escritura y la civilización sin escritura»².

Así pues, esta imparable carrera por hacerse con el poder, que proporciona el conocimiento a través de la información, supone la aparición de peligrosas amenazas o riesgos para los individuos, incapaces por sí mismos de controlar el ejercicio del poder a través del dominio de las tecnologías. Por tanto, si las ingentes posibilidades tecnológicas abren una puerta a la obtención de informaciones, se hace necesario articular los pertinentes mecanismos de control de dicha tecnología para evitar las vulneraciones de los derechos fundamentales, ya que si las tecnologías son sinónimo de poder, en cuanto control de la información, todo poder para ser democrático ha de ser susceptible de control. Como pone de manifiesto el Profesor PÉREZ LUÑO «en las sociedades informatizadas del presente 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»³.

Así, en este orden de cosas, el Estado ha de demostrar que sigue estando capacitado para cumplir su función tradicional de proteger a los ciudadanos, y en este sentido, se ha desarrollado en los últimos años el denominado «Derecho Informático» como rama específica

¹ DAVARA RODRÍGUEZ, M. A.: *De las autopistas de la información a la Sociedad Virtual*, Pamplona, 1996, pág.33 y 34.

² FROSINI: «Problemas jurídicos del desarrollo de la informática y de la información», *Revista de Derecho Comparada*, nº 5, 1981, pp.25-36.

³ PÉREZ LUÑO, A. E.: «Los Derechos Humanos en la sociedad tecnológica», en *Libertad informática y leyes de protección de datos personales*, AA.VV.: *Cuadernos y Debates*, nº 21, Madrid, 1990, pág.136.

del Derecho dedicada a proteger los derechos fundamentales frente a las vulneraciones producidas a través de los medios tecnológicos⁴.

II. LA PROTECCIÓN DE LA VIDA PRIVADA

Los Estados siempre han necesitado de la información para progresar siendo más poderosos cuanto más sea la información detenida. Si el Estado *orwelliano* ejercía un control totalitario gracias al monopolio de la información, el Estado que es sujeto del nuevo contexto global ha experimentado una transformación en las estructuras del poder que lo caracterizan y en sus funciones, a través de la descentralización y la difuminación de las fronteras entre lo público y lo privado. La globalización económica ha supuesto grandes cambios en la prestación de servicios, y así, el Estado tradicionalmente garante de los intereses generales vive la insuficiencia de capital propio para invertir en políticas sociales y requiere de la colaboración de otros sujetos para que complementen su oferta de servicios, iniciándose así un proceso de privatización de funciones, tradicionalmente públicas, que ya no tiene marcha atrás. La confusión entre intereses públicos y privados es evidente y ha provocado la comercialización o mercantilización de bienes tan relevantes como la libertad de expresión, la intimidad o la igualdad, por lo que el disfrute de muchos bienes ya no depende de los poderes públicos que pierden el control a favor de las grandes empresas y multinacionales, cuyas actividades en ningún caso son tan controlables como las instituciones públicas, pues no existen mecanismos de control del poder como garantía individual⁵.

⁴ PÉREZ-UGENA, M. Y PÉREZ-UGENA, A.: «Implicaciones constitucionales de las nuevas tecnologías», *Revista de Derecho Político*, UNED, nº 54, Madrid, 2002, pág.156, señalan que «la solución no parece estar tanto en potenciar el desarrollo de una rama del Derecho que estudie los aspectos jurídicos de la informática, como en incluir su estudio en las distintas ramas, sin que esto conlleve su desaparición. Así, la problemática jurídica que pueda plantear la actividad desarrollada a través de medios tecnológicos exige un planteamiento multidisciplinar desde la óptica el Derecho Constitucional, Administrativo, Civil, Penal, Laboral, Procesal, Mercantil, de la Filosofía del Derecho o la Sociología, entre otros».

⁵ El actual papel de los medios de comunicación está marcado por las nuevas tecnologías y éstos se han erigido en los auténticos protagonistas de la vida pública, hasta el punto de dirigir *de facto* el proceso político

Todo ello obliga a que el Estado asuma de forma decidida la protección de los individuos frente a la aplicación tecnológica, lo que supone la regulación de estas actividades a través de la intervención pública teniendo en cuenta sus beneficios pero también sus peligros. En otras palabras, el reto que se ha de afrontar y tratar de responder es la creación de un espacio apropiado para desarrollar de la mejor forma posible la Sociedad de la Información tanto para los Estados como para los ciudadanos, sin olvidar a los demás actores inmersos en el nuevo contexto informacional.

Así, debemos centrarnos en la situación en que se encuentran los ciudadanos como parte afectada por las nuevas tecnologías, potencialmente vulneradoras de sus derechos, de las que son sujeto pero también objeto, por lo que se requiere la creación de un entorno normativo y político adecuado que les garantice su plena integración en los procesos y relaciones propios de esta nueva realidad y la plena garantía de sus derechos fundamentales cuyo contenido y alcance queda determinado por la aplicación de las nuevas tecnologías⁶.

Así pues, sucede que las características de la nueva sociedad de la información ponen de relieve el problema de la protección de la vida privada, agudizado con el desarrollado de las autopistas de la información y de Internet, lo que obliga a replantear, tal como señala CAMPUZANO TOMÉ, «el tema de la protección de los datos personales», pues «no es que los nuevos medios electrónicos hayan modificado el concepto de privacidad, pero sí que han cambiado las formas en que éste puede ser protegido o puesto en peligro»⁷.

La protección que requiere la vida privada de los individuos responde al interés constitucional por construir la protección del individuo en trono al principio personalista que supone el reconocimiento de derechos «singulares» que responden a una situación histórica, social, económica o laboral, específica de la que nacen situaciones subjetivas que merecen ser reconocidas y tuteladas. En este sentido, el sistema de garantía constitucional de los derechos coloca al individuo en la posición central como un sujeto no considerado en abstracto sino en su marco personal condicionada histórica, social y materialmente, lo que determina que tenga unas nece-

⁶ En este sentido, LÓPEZ GARRIDO, D.: «La sociedad informatizada y la crisis del Estado de bienestar», *Revista de Estudios Políticos*, nº 48-49, 1985, pp.27-45.

⁷ CAMPUZANO TOMÉ, H.: *Vida privada y Datos Personales*, Madrid, 2000, pág.66.

sidades y demandas específicas. Y esto es lo que sucede con el derecho a la vida privada que tiene que ser garantizado dentro del marco constitucional como derecho configurado en un determinado contexto social configurado e influido por las nuevas tecnologías.

En este orden de cosas, la flexibilidad de las normas constitucionales permite su adaptación al devenir histórico, dotándolas de actualidad y de capacidad de respuesta a situaciones de amenazas concretas que se producen en nuestros días. Unas interpretaciones que adaptan las disposiciones establecidas y que se apoyan en cláusulas constitucionales que reconocen con carácter general la dignidad humana y el libre desarrollo de la personalidad como base y fundamento de los derechos fundamentales⁸.

La vida privada de las personas y, en definitiva, la libertad individual están en peligro ante el imparable y, en ocasiones, incontrolable, desarrollo tecnológico (medios de comunicación, técnicas de vigilancia, investigación genética, etc) que invade la privacidad sin que los titulares de esa vida privada puedan hacer nada, bien por la ineficacia de las garantías tradicionales bien porque la intromisión se lleva a cabo sin el conocimiento del afectado. Ante esta situación real, la respuesta no se puede hacer esperar y las soluciones jurídicas pasan por redefinir el derecho a la intimidad, completándolo con nuevas facultades y garantías, o por desarrollar a partir de la intimidad en sentido clásico, nuevos derechos fundamentales que permitan frenar esas intromisiones. Por tanto, las cuestiones que se han de abordar desde el poder público, a través de las políticas de información, se reconducen a dos. Por un lado, la actuación positiva de las Administraciones Públicas ha de potenciar el desarrollo y el acce-

⁸ De esta opinión JIMÉNEZ DE PARGA quien considera que «la piedra angular, base o fundamento principal, es el art.10.1º .E. [...] siendo las palabras clave «fundamento del orden político y de la paz». Estamos ante «unos principios constitucionales la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás» que al ser principios constitucionales suponen que todo el ordenamiento ha de interpretarse conforme a esos principios que son, además, directamente vinculantes». «Con estos principios constitucionales (constitucionalizados), de aplicación directa, y el apoyo de determinados derechos expresamente reconocidos en la Constitución de 1978, así como en Textos Internacionales, es posible extender la tutela a ciertos derechos de singular relieve e importancia en el actual momento de la Historia. Tal es el derecho fundamental de libertad informática», JIMÉNEZ DE PARGA, M.: «La refundamentación del ordenamiento jurídico» en *Persona y Derecho*, nº 44, 2001, pp.27-28.

so de todos los sectores y, por otro, ha de proteger a los ciudadanos posibilitando el control de la aplicación tecnológica. La seguridad de la información se convierte en una pieza clave en la construcción y desarrollo de una Sociedad de la Información para todos, pues sin seguridad no será viable la protección de los derechos fundamentales, ya que, obviamente, el control de nuestras informaciones personales requiere el punto de equilibrio entre las tecnologías y la tutela de nuestros derechos.

No obstante lo anterior, es necesario mencionar las intenciones, la ética y la responsabilidad de las personas, las instituciones, los gobiernos y de las sociedades en su conjunto, en este espacio global de las informaciones, de los flujos de datos, de las tecnologías avanzadas, del ciberespacio, de la intimidad y privacidad. Y es que no hay que olvidar que las nuevas tecnologías y su aplicaciones reportan beneficios, pues «Aunque las nuevas tecnologías naturalmente afectan a los derechos humanos de manera ambivalente, para bien y para mal, pueden ser favorables, por ejemplo las biotecnologías pueden impulsar el derecho a la vida y el derecho a la protección de la salud, pero pueden también dañar a ese mismo derecho a la vida, pueden dañar a la intimidad, pueden dañar el honor y la propia imagen, o pueden dañar el derecho al medio ambiente [...] Y si nos entramos en los derechos políticos, la situación es la misma, y podemos encontrarnos con impulsos positivos y con impulsos negativos»⁹.

Y es que las amenazas para la libertad y, en definitiva, para todos los derechos fundamentales dependen directamente de las intenciones de quienes detentan el poder tecnológico y no sólo obedecen al avance y progreso, pues por ejemplo países como Suecia que dispone los ficheros más ricos y mejor cruzados corren pocos riesgos de convertirse en un régimen policial y, sin embargo, la Gestapo realizó eficazmente su «trabajo» sin disponer de ficheros electrónicos interconectados¹⁰. Siendo manifiestamente claro en el ámbito de los datos sobre la salud, donde las cuestiones éticas adquieren mayor relevancia en cuanto que estamos ante datos especialmente sensibles. En el manejo de estos datos e informaciones concurren intereses dis-

⁹ PECES-BARBA, G.: «Los Derechos Fundamentales de naturaleza política y las nuevas tecnologías», *II Jornadas Parlamentarias de la Asamblea de Madrid*, «Parlamento y Nuevas Tecnologías», Madrid, 2002, pág.153.

¹⁰ NORA, S. y MINC, A.: *La informatización de la sociedad*, Trad. García de Pruneda, P. Y Ruza, R., México, 1980, pág.96.

tintos a los del paciente que, evidentemente, pueden colisionar con éstos y por eso la confidencialidad de estos datos personales ha sido regulada en la legislación sanitaria, que trata de proteger el historial clínico del paciente cuya propiedad suscita serios debates que abarcan cuestiones con dimensiones éticas, morales y jurídicas. En este sentido, el concepto de confidencialidad concilia el secreto médico profesional (juramento hipocrático) y la protección de los datos sobre la salud como derecho fundamental de los ciudadanos.

En definitiva, la recopilación de datos es una actividad desarrollada tanto por los vigilantes públicos como privados, favorecidos por las aplicaciones tecnológicas que aumentan las posibilidades de adquisición, pero, también, el almacenamiento, recuperación y procesamiento de los mismos. El final de este proceso nos conduce a las bases de datos que pueden pertenecer a los gobiernos, a las empresas o a otras organizaciones, en las que se almacena la información de forma sistemática y, en teoría, segura. Estas bases se crean con unos fines específicos y, por eso, los datos recopilados y almacenados responden a objetivos concretos, lo que supone que su captación obedece, generalmente, a respuestas a preguntas determinadas. Por tanto, la información se obtiene mayoritariamente mediante la cesión libre y voluntaria de datos por su titular original y, en menos ocasiones, de forma encubierta. Así, los operadores de las bases de datos consideran a éstos un producto comercial, objeto de venta, a diferencia por ejemplo de los informes en poder de los Servicios de Inteligencia, encontrando en la realización de estas operaciones económicas algunos obstáculos necesarios para la protección de los derechos de las personas provenientes de las leyes y de las regulaciones estatales, así como de los códigos de conducta de las propias empresas. Estas normas privadas de autorregulación no tienen carácter obligatorio para las empresas que a través de ellas se comprometen a practicar una política de respeto a la vida privada y a la confidencialidad de los datos personales, por lo que los afectados no pueden solicitar una reparación del daño causado por su incumplimiento.

Cualquier dato de naturaleza personal reviste importancia aunque, a simple vista y por sí mismo, no revele ninguna información personal relevante. En este sentido, los datos sensibles resultan más protegidos que otros porque su vulnerabilidad es evidente (datos raciales, salud o genéticos), pero otros no gozan de una protección tan fuerte, aún cuando su manipulación y tratamiento indebidos constituyen graves amenazas para la vida de las personas, pues, a través del emparejamiento de datos aparentemente inocuos pueden elaborarse perfiles detallados de las personas. Tal como pone de mani-

fiesto CAMPUZANO TOMÉ «Supone el cruce o triangularización de dos o más datos contenidos en diferentes bases, mediante el cual puede llegar a obtenerse una información realmente detallada de los sujetos. La doctrina nos muestra un claro ejemplo: en un estudio realizado se pidieron las bases de datos con las fichas laborales de los trabajadores de todo un hospital, con la excusa de hacer un pequeño estudio de perfiles. El hospital entregó esa información eliminando los campos personales como la dirección, el teléfono y el nombre. Así, a partir de los datos existentes en los registros, las fechas de nacimiento y el código postal y cruzando esa información con los datos del censo, fue posible averiguar la identidad de más del setenta por ciento de los trabajadores de ese hospital»¹¹.

EL control resulta fundamental para lograr la protección de la vida privada, pues permite controlar las informaciones que versan sobre nosotros mismos y sobre este elemento se ha elaborado un nuevo derecho fundamental para garantizar la privacidad de las personas en el contexto tecnológico¹².

En este orden de cosas, los datos personales integran la vida privada de las personas, pues nuestras vivencias van generando datos que describen nuestro paso por el mundo, y esos datos son transmitidos cuando se pretenden contar nuestras acciones o acontecimientos personales. Así, si la acción es de naturaleza privada pertenece a quien la realiza, pudiendo excluir a cualquier otro de su conocimiento, lo que implica controlar los datos que dicha acción genera. Y es que el derecho a la vida privada no es sólo un derecho negativo en cuanto derecho a que no se divulguen o hagan públicos aspectos particulares de la propia vida, lo que en todo caso resulta

¹¹ CAMPUZANO TOMÉ, H.: *Vida Privada ... cit.*, pág.61.

¹² Para una definición de la vida privada sirva la reciente Sentencia del Tribunal Europeo de Derechos Humanos, STEDH, de 28 de enero de 2003, asunto *Peck* contra el Reino Unido, con remisión a la STEDH de 2001, P.G. y G.H. contra el Reino Unido, donde se declara que «vida privada es un término amplio no suceptible de una definición exhaustiva. El Tribunal ya ha decidido que elemento como la identificación del género, nombre, orientación y vida sexual son elementos importantes de la esfera personal protegidos por el artículo 8. El artículo protege también un derecho a la identidad y al desarrollo personal, y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el exterior y eso puede incluir actividades de naturaleza profesional o de negocios. Por lo tanto, existe una zona de interacción de la persona con los demás, incluso en un contexto público, que puede entrar en el ámbito de la vida privada».

insuficiente, sino que comprende una dimensión positiva que permite desarrollar libremente la propia personalidad. Y ese contenido positivo se articula en forma de derecho de control sobre los datos relativos a la propia persona, la llamada «libertad informática» o «derecho a la autodeterminación informativa» que como derecho derivado de la dignidad de la persona permite el libre desarrollo de la personalidad¹³.

En el año 2000 el Tribunal Constitucional reconoce abiertamente un nuevo derecho fundamental autónomo que podemos definir como un derecho personalísimo con autonomía respecto a otros derechos como la intimidad o privacidad, la imagen, el honor o la identidad personal, pues a través de su reconocimiento se persigue la protección de la libertad de los individuos para determinar por sí mismo, cuándo, cómo y hasta qué punto se comunica a terceras personas información referida a ellos¹⁴.

El Tribunal Constitucional declara que ambos derechos fundamentales, la intimidad y la protección de datos o autodeterminación informativa difieren en su función, objeto y contenido. Mientras la función del derecho fundamental a la intimidad es la de proteger, frente a cualquier invasión, el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, excluyendo por tanto ciertos datos del conocimiento ajeno, para resguardar la vida privada, el derecho a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, garantizando por tanto un poder de disposición sobre esos datos, previo conocimiento de qué datos poseen los terceros, quiénes los poseen y con qué fin e imponiendo a los poderes públicos la prohibición de que se conviertan en fuentes de información sin las debidas garantías y de que prevengan los riesgos que puedan derivarse del acceso o divulgación indebida de esa información. **El objeto del derecho fundamental a la protección de datos es más amplio que el del derecho a la intimidad y extiende su garantía no sólo a la intimidad, sino a la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida**

¹³ SSTC 254/1993, 20 de julio y 143/1994, 9 de mayo.

¹⁴ STC 292/2000, 30 de noviembre. Este derecho está regulado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

privada y están unidos al respeto de la dignidad personal, como el derecho al honor, y al pleno ejercicio de los derechos de la persona, ampliando la garantía constitucional a los datos relevantes o que tengan incidencia en el ejercicio de cualesquiera derechos de la persona. Su objeto no se reduce sólo a los datos íntimos de la persona, relativos a su vida privada o íntima, sino a cualquier tipo de dato personal, sea o no íntimo.

Desde el punto del vista del contenido, **mientras el derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido, el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos de hacer que no se contienen en el derecho a la intimidad y que sirven a la función esencial de garantizar a la persona un poder de control sobre sus datos personales: el derecho a que se requiera el previo consentimiento para la recogida y uso de dichos datos y el derecho de saber y ser informado sobre el destino y uso de dichos datos y el derecho de acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles pueda ese tercero recabar y que permite también al individuo saber quién posee estos datos personales y para qué, pudiendo oponerse a esa posesión o uso, facultándole para consentir la recogida, la obtención y el acceso a estos datos, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero, sea el Estado o un particular.**

III. LA NECESIDAD DE OBTENER Y TRATAR LA INFORMACIÓN

El Estado siempre ha necesitado recopilar informaciones para detentar el mayor conocimiento posible para gestionar los asuntos públicos con eficacia, para controlar las informaciones tanto hacia dentro como hacia fuera de sus fronteras y presentarse como un sujeto fuerte y seguro ante sus ciudadanos y ante las demás naciones. Así pues, el Estado siempre ha sido considerado el mayor enemigo de la intimidad de las personas, pues en cuanto organización política desarrollada requiere de una administración para asuntos relacionados con la recaudación del dinero, con la guerra y, desde luego, con la seguridad. Siendo estas las principales actividades del Estado, ejer-

cidas a través de sus administraciones, ello exige contar con grandes cantidades de información cuanto más detallada mejor¹⁵. Y es que el desarrollo de las sociedades cada vez más complejas determina la transformación de la Administración a lo largo de los dos últimos siglos, por lo que en este siglo XXI ha visto incrementadas sus funciones de modo que se erige como un actor determinante para alcanzar el desarrollo social, económico, científico y tecnológico. El Estado procurador de bienes y servicios asume, junto a las funciones públicas de seguridad, interna y externa, y las funciones recaudatorias, la gestión de intereses y tareas cada vez más complejas, para lo que se sirve de la aplicación de las tecnologías de la información y las comunicaciones¹⁶.

Y es que el desarrollo tecnológico ha de orientarse para mejorar la vida de las personas; facilitando el trabajo, fomentando la salud, con un mejor aprovechamiento de las energías, con respeto a la naturaleza, generalizando la educación, y la cultura y, como no, contribuyendo al crecimiento económico. Por eso, hay que poner mucho celo, pues «la innovación técnica no ha de poner en peligro el ejercicio de derechos fundamentales sino facilitarlos [...]»¹⁷.

Las inmensas posibilidades de recopilar informaciones, preferentemente de carácter personal, que ofrecen las tecnologías, otorgan un control «casi global» de los ciudadanos, tal como sucederá con el proyecto que, en diciembre de 2002, presentó el Pentágono, recogiendo sus intenciones de construir un gran sistema de vigilancia con el nombre de *Total Information Awareness* (Conocimiento Total de la Información», una ingente red de datos que permitiría rastrear la huella que cualquier ciudadano deja al efectuar transacciones bancarias, alquileres de vehículos, compras con tarjeta, contratos de suministros, etc. Ya en 1787 BENTHAM sugiere un modelo de prisión «Panóptico» donde todos los reos pueden ser observados durante veinticuatro horas por un carcelero situado en lo alto del edificio sin tener que mostrar su cara (vigilancia total). Esto es ficción, pero la idea que subyace se puede trasladar a la realidad cuando los asistentes a la final

¹⁵ RIVERO, R.: *El Estado vigilante*, Madrid, 2000.

¹⁶ JARQUE URIBE, C.: «Aplicación de las Tecnologías de la Información y las Comunicaciones en las Administraciones Públicas». *Proyecto de Innovación y Modernización en las Administraciones Públicas*, Madrid, 2000: MARTÍNEZ DÍEZ, R.: «El proceso de informatización de la Administración Pública española», *Documentación Administrativa*, nº 200, pp.133-162.

¹⁷ LAFONTAINE, O.: *La sociedad del futuro*, Madrid, 1993, pág.78.

del Campeonato Nacional de Fútbol Americano celebrada en Tampa en febrero de 2000, no se percataron de una cámara de televisión encargada de grabar la entrada de todo, uno a uno, en el estadio. La policía de Florida había puesto en marcha un prototipo de vigilancia biométrica consistente en comparar los rostros de estos miles de personas con los de delincuentes y sospechosos.

El prestigioso Profesor de Ciencia Política en la Universidad de Toronto, WHITAKER, alertó sobre la vigilancia y las amenazas a la intimidad, admitiendo que «la defensa de la intimidad ha empezado a carecer de sentido desde el momento en que cada transacción, cada contacto que realizamos con una nueva tecnología puede ser rastreado por alguien. Yo no digo que alguien nos vigila a cada momento, pero la tecnología permite que quien quiera hacerlo lo haga»¹⁸.

En este sentido, en las sociedades actuales, ya sea por motivos de seguridad o por motivos económicos para conocer los gustos y hábitos del consumidor o usuario, proliferan de forma imparable la instalación de cámaras, algoritmos de reconocimiento, bases de datos, herramientas de biométrica, ya sea por la policía, Administraciones, bancos, comercios, padres, empresarios, para la protección de sus intereses¹⁹. Por tanto, nos encontramos ante la existencia de innumerables fuentes de información públicas y privadas desperdigadas que de ser reunidas conformarían una gran red de vigilancia a disposición de las autoridades que quisieran utilizarla.

Así las cosas, las informaciones de carácter personal del ciudadano que es un usuario y un consumidor interesan no sólo a las administraciones sino también al sector privado, con lo que los datos personales se ha convertido en un bien sumamente codiciado en la Sociedad de la Información, precisamente por la información que de ellos se extrae con gran relevancia para la vida política y económica. Por tanto, estos datos tan codiciados son recopilados por el Estado, pero también por las empresas públicas y privadas que los requieren para un funcionamiento más rentable y que por su poder tecnológico superan, en ocasiones, al propio Estado, tradicionalmente visto como el Gran Ojo Público.

¹⁸ WHITAKER, R.: *El fin de la privacidad*, Barcelona, 1999.

¹⁹ ABA CATOIRA, A.: «La videovigilancia y la garantía de los derechos individuales: su marco jurídico», *Anuario da Faculdade de Direito da Universidade da Coruña*, nº 7, 2003.

Así pues, la importancia que revisten estos datos, de ahí la necesidad de obtenerlos, se debe a la valiosa información que desprenden una vez interconectados y ser objeto de un adecuado tratamiento. Por ello son solicitados, mayoritariamente, por las administraciones estatales a través de los diferentes Ministerios. En este orden de cosas, el Ministerio de Justicia los solicita para la configuración de los ficheros de penados y rebeldes; Defensa para la configuración de los ficheros de inteligencia militar; Economía y Hacienda para elaborar los ficheros tributarios; Interior para los ficheros policiales, el Documento Nacional de Identidad, lucha antiterrorista, búsqueda de personas desaparecidas, etc.; Trabajo y Seguridad Social para registrar a las personas que están en paro, afiliadas a la Seguridad Social o las que sufren minusvalías o Sanidad para confeccionar los históricos clínicos. Esta cantidad de información en manos del Estado convierte a sus administrados en seres absolutamente transparentes controlados hasta la saciedad.

Pero el Estado no es el único interesado en obtener la mayor cantidad posible de informaciones que le permitan ejercer su autoridad y alcanzar la máxima eficacia en sus actuaciones. Las empresas públicas o privadas como Bancos, Cajas de Ahorro, Compañías de Seguros, empresas de informes comerciales de morosos e insolventes, agencias matrimoniales, agencias de detectives privados, empresas de publicidad comercial por correo, editoriales, o los simples centros de trabajo, se hacen con tal cantidad de datos personales, en su mayoría, cedidos voluntariamente por los ciudadanos, a diferencia de lo que ocurre cuando son solicitados por las administraciones, con el fin de establecer alguna relación comercial o económica. El hecho de que no se trate de datos recabados obligatoriamente hace que la persona a que se refiere dicha información personal, ceda sus datos sin resquemores sin tener en cuenta que esos datos aislados en manos de los poderosos agentes privados se convierten en una seria amenaza para sus derechos fundamentales, incluso más que cuando es el Estado quien detenta esa información. A ellas se suman otras organizaciones que, aún no siendo Administración Pública ni empresas, recaban estos datos, como es el caso de las asociaciones deportivas o culturales, así como las confesiones religiosas, partidos políticos o sindicatos²⁰.

²⁰ VELÁZQUEZ, R.: *La protección jurídica de datos personales automatizados*, Madrid, 1993.

En la realización de muchas de las funciones estatales se constata la notable dificultad de los ciudadanos para controlar dichas actuaciones con el fin de evitar excesos lesivos de los derechos y libertades. Por ejemplo, cuando en prevención de actos que atenten contra la seguridad pública, uno de los conceptos indeterminados utilizados en el establecimiento de límites de derechos y libertades, el poder coactivo estatal supone una grave amenaza para la libertad individual sin que sea posible establecer un procedimiento previo, lo suficientemente formalizado y detallado, como para asegurar un control eficaz de los posibles excesos. Es lo que sucede con las diligencias policiales de identificación en cuanto medidas realizadas por las autoridades policiales y administrativas con la finalidad de obtener los datos personales de un individuo, pero que pueden tener como consecuencia el contraste de esos datos necesarios para prevención del delito con otros datos que constan en los archivos y registros policiales. Ciertamente hay que poner mucho cuidado para que tales medidas de control y vigilancia de las personas no se acaben convirtiendo en ámbitos estatales exentos de control y ajenos al principio de responsabilidad, presupuesto esencial del Estado Democrático de Derecho.

III.1º. ACTUACIONES ESTATALES CON INCIDENCIA EN LA INTIMIDAD

Son numerosos los ámbitos en los que el Estado interviene recopilando datos sobre los ciudadanos por diversos motivos que presiden sus actuaciones, siendo la cesión de información personal para la identificación de las personas una obligación que provoca grandes recelos entre los ciudadanos. En este sentido, la Comisión Europea de Derechos Humanos ha declarado que ninguna norma del Convenio Europeo de Derechos Humanos prohíbe el uso de números de identificación personal, por lo que habrá que regular qué datos se pueden recabar y qué uso se les puede dar para no vulnerar la intimidad de las personas²¹.

En España la implantación de un número como identificación personal, conocido como Documento Nacional de Identidad (D.N.I.),

²¹ Decisión de la Comisión Europea de Derechos Humanos de 11 de diciembre de 1985, asunto *Lundwall* contra Suecia, nº 3.

se estableció en normas preconstitucionales, primero a través del Decreto de 2 de marzo de 1944 que se modificó por Decreto 196/1976, de 6 de febrero. Esta norma gubernamental, anterior a la Constitución de 1978, establece que el Documento Nacional de Identidad es «el único documento público que acredita la auténtica personalidad de su titular, constituyendo el único y exclusivo justificante completo de la identificación de las personas» (art.1.1º). Es un documento «imprescindible» para acreditar oficialmente la personalidad del titular, siendo «obligatorio» (art.1.2º y 3º).

Con la entrada en vigor de la Constitución se modificó esta regulación preconstitucional por el Real Decreto 1245/1985, de 17 de julio y por Ley Orgánica de 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, para adecuarla a las previsiones constitucionales. Así, se suprimió el carácter «único y exclusivo» de este documento para justificar la identidad de las personas, y, tras declarar que el Documento por sí solo tiene suficiente valor para la acreditación de la identidad, se reconoce la posibilidad de hacerlo a través de otros documentos (art.9.1º y 20.2º).

Así las cosas, no se discute la constitucionalidad de la existencia del Documento sino las formas de solicitar la identificación de las personas y la forma en que se viene realizando. Por tanto, las identificaciones realizadas por las Fuerzas de Seguridad e incluso por terceras personas y los lugares donde se llevan a cabo han motivado el pronunciamiento del Tribunal Constitucional contenido en la STC 341/1993, resolviendo las dudas planteadas sobre la inconstitucionalidad de la norma.

Por lo que respecta a los datos que han de figurar en el Documento la norma de 1976 señala que constarán los datos personales, fotográficos y dactilares que evidencien la personalidad del titular, así como el domicilio, entendiendo por datos personales el nombre y apellidos, el nombre de los padres, sexo, fecha y lugar de nacimiento. Por su parte, la Ley Orgánica de Protección de Seguridad Ciudadana establece que han de constar como datos, la fotografía, la firma y los datos que se determinen reglamentariamente sin que puedan ser relativos a la raza, religión, opinión, ideología, afiliación política o sindical o creencias (art.9.2º).

La obligación de ceder estos datos como las huellas dactilares ha suscitado duras críticas por entenderse que «la averiguación por el Estado de algo tan personal y único como las huellas dactilares y su almacenamiento respecto de todos los ciudadanos, es de todo punto inconstitucional, debiéndose destruir todos los datos dactilares de

personas no delincuentes»²². Al respecto creemos que la obtención y almacenamiento de las huellas dactilares supone una evidente intervención en la intimidad de las personas, pero la cesión de esta información resulta necesaria para la prevención y sanción de los delitos, aunque, obviamente, el máximo respeto de la intimidad se lograría consignando el carácter no obligatorio de este Documento.

El Número de Identificación Fiscal (N.I.F.) regulado por el Real Decreto 338/1990, de 9 de marzo, y por la Orden Ministerial, de 14 de marzo del mismo año, en desarrollo del anterior, presenta más dudas en torno a su constitucionalidad, pues, presuntamente, supone la vulneración del derecho a la intimidad del art.181º, así como del 18.4º, al existir dudas sobre el uso que se da a la información obtenida a través de operaciones identificadas con el Número de Identificación Fiscal, y, por consiguiente, suponer la lesión del derecho de autodeterminación informativa. Recordemos que este Número de Identificación se configura añadiendo al número del Documento Nacional de Identidad una letra correspondiente a un código de verificación, limitándose su uso a operaciones de «naturaleza o con trascendencia tributaria» del sujeto identificado. El derecho a controlar las informaciones que nos afectan se ve lesionado cuando la utilización de la información no es aquella para la que se obtuvo dicha información, y que justifica su cesión por parte de los ciudadanos.

El Tribunal Constitucional ha declarado que no puede entenderse vulnerada la intimidad de las personas por la exigencia de transmitir información sobre actividades desenvueltas en el tráfico económico y negocial. Unas actividades que tienden a desarrollar en el ámbito de relación con terceros y a estar sometidas a fórmulas específicas de publicidad en aras de la seguridad jurídica y de la transparencia en el tráfico económico, de ahí que sólo con extremada dificultad puedan calificarse como reservadas, en el sentido antes descrito, típico del juego del derecho a la intimidad (la intimidad como ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario según las pautas de nuestra cultura para mantener una calidad mínima de la vida humana). Se puede aceptar que algunos aspectos sobre los que ha de versar la información inciden sobre el ámbito protegido del derecho a la intimidad, pero no por eso se puede rechazar *a priori* la imposición de cargas informativas.

²² RUIZ MIGUEL, C.: *La configuración constitucional del derecho a la intimidad*, Madrid, 1992, pág.152.

El Tribunal Constitucional concluye que el N.I.F. no supone un riesgo para la protección de datos personales, «no porque sea imposible, sino porque las cautelas establecidas por el ordenamiento jurídico para su utilización lo conjuran»²³.

El citado Decreto de 1990 busca fórmulas de lucha contra el fraude fiscal mediante instrumentos de seguimiento y control de las actividades que realicen los sujetos obligados al pago de tributos. En este sentido, la obligación de tener el N.I.F. para intervenir en relaciones económicas o tributarias se rige por criterios fiscales, pues busca el control en materia tributaria. Por tanto, descartada la inconstitucionalidad de su imposición el problema reside en determinar la legitimidad de una norma que posibilita conocer determinada información fiscal, que usada de forma indebida permita conocer la vida privada de las personas sin justificación.

El derecho fundamental a controlar las informaciones personales obliga a las normas a establecer garantías adecuadas frente al tratamiento técnico de las informaciones, cuya recopilación autoriza, potencialmente lesivo de la vida privada. La norma en cuestión no desconoce las garantías, pues los principios de protección de los datos personales que rigen la recopilación, almacenamiento y tratamiento de los mismos, son respetados al establecerse la legitimidad de la recogida, la adecuación de la información obtenida a las finalidades perseguidas, el deber de reserva sobre los datos personales, la seguridad de los archivos, o el principio del consentimiento para la cesión de éstos.

Lo que no puede obviarse es que tanto la regulación de la identificación personal como fiscal adolecen de falta de rango legal, pues, dejando al margen que ningún precepto constitucional apoya la imposición de estos documentos, los aspectos sustanciales relativos al D.N.I. quedan establecidos en un Real Decreto y en una Orden Ministerial, mientras que la Ley Orgánica del 92 sólo regula aspectos tangenciales y, más aún, su art.9 no tiene rango de ley orgánica. En lo tocante al N.I.F. éste se aprobó por Ley 33/1987, de 23 de diciembre que acompaña a la Ley de Presupuestos para 1988 (art.113.1º) y se regula en Real Decreto. Así las cosas, las garantías formales exigidas para la regulación y desarrollo de los derechos fundamentales, es decir, el respeto de los artículos 53.1º

²³ STC 143/1994, 9 de mayo.

y 81 de la Constitución, se vulnera a través de una intervención en el ámbito constitucionalmente protegido del art.18 de la Constitución, que además no lleva a cabo el legislador y se justifica en la protección de intereses constitucionales que no son derechos fundamentales²⁴.

Lógicamente, las críticas que se efectúan contra la utilización de un único número de identificación personal, como son el D.N.I. y el N.I.F., se dirigen al control que posibilitan, pues se «produce una multiplicación de esta capacidad de vigilancia y una disminución de la calidad de vida democrática». Y esto es así hasta el punto que «algunos países, quizás con mayor frescura democrática, en el sentido que pudieron debatir en un ambiente distinto del español, se decidieron a introducir en su Constitución, y nada menos que en su Constitución, como una práctica inconstitucional, la prohibición de utilizar un número nacional único de identificación de los ciudadanos»²⁵. Tal como señala LUCAS MURILLO «En todo caso es significativo que siendo los números de identificación personal uno de los problemas más debatidos en el marco de la protección de datos personales, habida cuenta de los riesgos que pueden acarrear para la autodeterminación informativa, el Tribunal Constitucional pase por alto —más bien descarte— esa potencial peligrosidad. Naturalmente, lo que procede es justamente lo contrario: de ahí que se proponga la introducción de fuertes límites a la utilización de este instrumento, pues no se desconoce su idoneidad para centralizar la información personal diseminada en ficheros automatizados públicos y privados»²⁶.

En este orden de cosas, el modelo portugués parece más adecuado y respetuoso con los derechos fundamentales, pues establece dos claves de identificación distintas para lo que se denomina el Registro de Identificación Civil y el Registro de Identificación Fscial, y otra clave distinta para la Seguridad Social o para todas las mutualidades o Instituciones que cubren riesgos sociales.

²⁴ ABA CATOIRA, A.: *La limitación de los derechos fundamentales en la jurisprudencia del Tribunal Constitucional español*, Valencia, 1999; y el primer capítulo de *La limitación de los derechos por razón del sujeto*, Madrid, 2001.

²⁵ MARTÍN PALLÍN, J. A.: «Intimidad, privacidad y protección de datos en la nueva L.O. 15/1999», *XIV Encuentros sobre Informática y Derecho*, 2000.

²⁶ LUCAS MURILLO, P.: «La construcción del derecho a la autodeterminación informativa», *Revista de Estudios Políticos*, n° 104, 1999, pág.45.

En último lugar poner de manifiesto que el Proyecto de Ley sobre Firma Electrónica presentando por el Gobierno para su tramitación el 20 de junio de 2002, regula el Documento Nacional de Identidad Electrónico que se erige en un certificado electrónico reconocido, llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. La Ley fija el marco normativo básico; acreditar la identidad de su titular en cualquier procedimiento administrativo y permitir la firma electrónica de documentos, remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico. Además, el 11 de julio el Gobierno, en Consejo de Ministros, aprobó el Real Decreto 896/2003, por el que se regula la expedición de un nuevo pasaporte que facilita las relaciones de los ciudadanos con la Administración a través de la implantación de las nuevas tecnologías, que contendrá la foto y firma electrónica con el fin de que sea apto para la lectura digital. Esta decisión obedece a «motivos de seguridad y adaptación a la normativa europea e internacional». Los pasaportes actuales servirán hasta su fecha de caducidad para viajar a todos los países excepto a Estados Unidos que desde el 1 de octubre obliga a que los extranjeros, a los que no se exige visado, cuenten con un pasaporte digital, siguiendo las medidas de seguridad establecidas tras el 11-S.

III.2º. EL RESPETO A LA VIDA PRIVADA EN LAS EMPRESAS

La protección de la vida privada adquiere especial relevancia en el marco de las relaciones laborales, donde se hace necesario controlar el tráfico de informaciones a las que se accede y que son tratadas bajo el interés legítimo por utilizar las enormes ventajas que proporciona el tratamiento automatizado de datos personales para aumentar la eficacia en la gestión del personal. Y es que, tal como afirma la doctrina, existen ciertas características de la relación laboral y funcionarial que dotan de trascendencia al tratamiento de datos y convierten a la misma en especialmente sensible a los peligros derivados de la informática. Su perdurabilidad, que hace importante la conservación de los datos; su carácter personal, que hace más complejo el tipo de datos a considerar; la diversidad del escenario para los que pueden ser relevantes y, en fin, el elevado número de trabajadores y funcionarios a los que se requiere información²⁷.

²⁷ Sentencia del Tribunal Superior de Justicia de Cantabria, Sala de lo Contencioso-Administrativo, sección única, de 10 de enero de 2003, Fundamento de Derecho 2º.

Existe un acuerdo unánime sobre la necesidad de que el ordenamiento nos proteja de los abusos cometidos en el tratamiento informático de nuestros datos personales que permiten la elaboración de perfiles de consumo y de conducta. Esta protección deparada por el ordenamiento resulta insuficiente, pues las normas de protección de datos adolecen de una deficitaria protección frente a las actuaciones provenientes del sector privado al dedicarse preferentemente al control de las actuaciones públicas. No obstante, en ocasiones se relaja esta protección, es decir, se relaja el control del cumplimiento de las medidas de protección, pues no son pocos los casos que saltan a la opinión pública sobre imprudencias que hacen que se amontonen los expedientes en las mesas de los juzgados, lo que permite leer el nombre de los imputados y el delito, que se encuentren en la basura los historiales clínicos o que en los ordenadores de la Administración se puedan cruzar numerosísimos datos.

Tal como se ha indicado las empresas realizan continuas medidas de control sobre los trabajadores utilizando distintas técnicas de vigilancia que los convierten en seres transparentes fácilmente controlables para su empleador. La generalización de esta vigilancia ha supuesto que se hayan resuelto judicialmente conflictos derivados del uso de datos personales de los trabajadores por un empresario, en cuanto que se despidió a los trabajadores en base a informaciones obtenidas a través de su vigilancia.

Así, en STC 11/1998 se resuelve un supuesto en el que la empresa utilizó datos relativos a la afiliación sindical de sus trabajadores, que obraban en su poder para proceder al descuento de las cuotas sindicales, para retener determinadas cantidades a los huelguistas. Estos trabajadores perdieron el control de sus datos personales relativos a su afiliación sindical y, por tanto, la empresa vulneró su derecho fundamental de libertad informática o autodeterminación informativa al utilizar ese dato sensible que se le proporcionó para una finalidad determinada y lícita radicalmente distinta. Asimismo, en STC 202/1999 se estudió la constitucionalidad de una base de datos en la que se registraron todas las bajas por incapacidad temporal de los trabajadores extendidas por los facultativos de la Seguridad Social, que se había creado sin el consentimiento expreso de los afectados, vulnerando así el art.18 de la Constitución.

La sentencia se pronunció a favor del empleado siguiendo lo dispuesto en el art.8 del Estatuto de los Trabajadores «sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares cuando sean necesarios para la protección del

patrimonio empresarial y el de los demás trabajadores, dentro del horario y del centro de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia, del centro de trabajo, de otro trabajador de la empresa, siempre que sea posible». Por tanto, las inspecciones que supongan el conocimiento de circunstancias de la vida privada de las personas y, por consiguiente, un tipo de vigilancia, sólo se podrán realizar respetando las garantías legales y la exigencia de justificación.

Otra de las medidas de vigilancia a las que recurren cada vez más los empresarios es el control de las comunicaciones, específicamente de Internet, en el lugar o puesto de trabajo. Esta cuestión adquiere cada día mayor relevancia siendo ya numerosos los despidos por causa de la inadecuada o indebida utilización del correo electrónico y de Internet. Evidentemente, este uso de las nuevas tecnologías con fines lúdicos o personales nos sitúa de lleno en el ámbito de la realización de los derechos fundamentales en el contexto tecnológico, pues colisionan los derechos de las dos partes, ya que el empresario ve dañado su poder o derecho de organizar y dirigir su empresa y, por consiguiente, la actividad de sus trabajadores y los trabajadores encuentran afectado su derecho a la intimidad y al secreto de las comunicaciones.

Así las cosas, cabe recordar que el empresario tiene reconocido el poder de dirección del empresario sobre la actividad de los trabajadores a su servicio, pudiendo adoptar las medidas que considere oportunas en orden a la vigilancia y control del cumplimiento por los mismos de sus obligaciones y deberes laborales (art.20 del Estatuto de los Trabajadores). Sin embargo, nada se dice sobre la forma en que el empresario puede realizar dicho control, lo que provoca polémicas entre los empresarios y sindicatos que no comparten la forma de ver y entender esta vigilancia.

Todas estas cuestiones suscitadas al pie del desarrollo tecnológico requieren de una adecuada respuesta legal, pero a la espera de que ésta se produzca contamos con una serie de resoluciones judiciales dictadas sobre la utilización indebida de las nuevas tecnologías por el trabajador y sobre todo acerca de los medios de investigación y control que puede utilizar el empresario para depurar las conductas de sus trabajadores. Si nos preguntamos por las soluciones judiciales hemos de concluir que las sentencias no siguen una línea continua sino que son dispares, lo que hace imposible, por ahora, establecer una respuesta uniforme, si bien si que pueden extraerse dos conclusiones bien definidas.

En primer lugar, que no toda utilización indebida del correo electrónico o de Internet constituye causa de despido, sino sólo aquella que constituya un incumplimiento grave y culpable de las obligaciones laborales del trabajador. Y la segunda no es otra que la constatación de la ausencia de una regulación sobre la utilización del correo por los trabajadores y sindicatos para fines ajenos al estricto cumplimiento de sus deberes laborales y la forma de controlar su posible utilización indebida por parte de la empresa.

Lógicamente, tal como suele suceder con todas las cosas, lo más adecuado para los intereses de ambas partes es la búsqueda del equilibrio, lo que parece ser el objetivo de la Unión Europea, pues la regulación de la materia se encuentra en la actualidad en el seno de la Comisión. Con el fin de acabar con la tensión que se produce por la vigilancia del comportamiento de los trabajadores en su condición de usuarios del correo electrónico facilitado por la empresa, la Comisión entiende que toda correspondencia, incluida la del correo electrónico, goza del derecho a la protección de la vida privada, reconocido en los Tratados Internacionales y, especialmente, en la Carta Europea de Derechos Fundamentales. Por ello, la Comisión propone que la vigilancia se efectúe de forma transparente, consultando a los sindicatos, sin que los empresarios estén autorizados a abrir el correo electrónico u otros ficheros privados, aunque no hayan autorizado su utilización privada por parte de los trabajadores.

En este sentido, en busca de una solución algunos sindicatos han firmado acuerdos bilaterales con las empresas, tal como hicieron Comisiones Obreras y el Barclays Bank acordando que la empresa dotará al sindicato de una cuenta de correo con determinados requisitos de extensión y cantidad de memoria utilizada, comprometiéndose a respetar la confidencialidad de las comunicaciones. Como señala MORALES PRATS las empresas están obligadas a informar a sus trabajadores de que el correo es una herramienta de trabajo y, por tanto, propiedad de la empresa, y han de definir el uso normal y cotidiano del mismo tal como resulta aceptado por la empresa. Cuando la empresa haya cumplido esas dos obligaciones habrá que establecer las medidas de control respecto a las que existen dos líneas de discusión. Por una parte, los partidarios de un control intenso consideran al correo como una herramienta de la empresa que ha de ser totalmente controlable por el empresario, por lo que defienden la posible intervención y visualización de los contenidos de los correos, y, por otra parte, los que defienden posturas más flexibles buscan el equilibrio, por lo que defienden que el empresario puede ordenar la forma y los límites del control, ya sea con una norma o por

Convenio Colectivo o acuerdos de empresa, pero no los contenidos, argumentando que así se salvaguarda la privacidad pero se permite controlar a la vez el uso indebido²⁸.

En Francia, la Sala de lo Social del Tribunal Supremo, se ha pronunciado claramente al respecto, siguiendo la línea establecida por la Unión Europea. Así, en una Sentencia de 2 de octubre de 2001, se pronuncia sobre la naturaleza jurídica del correo electrónico entendiéndose que éste goza de la protección otorgada a la correspondencia, papel y, por tanto, está protegido por el denominado secreto de la correspondencia. «El trabajador tiene derecho, incluso en el tiempo y lugar de trabajo, al respeto a la intimidad de su vida privada; ésta implica en particular el secreto de la correspondencia. El empresario no puede, sin violar esta libertad fundamental, investigar los mensajes personales emitidos por el trabajador y recibidos por él, gracias a un útil informático puesto a su disposición para su trabajo, incluso en el supuesto en que el empresario hubiera prohibido una utilización no profesional del ordenador». El conflicto surgió tras el despido de un trabajador alegando la empresa que éste utilizaba los recursos informáticos de la misma, entre ellos el correo electrónico, para sus asuntos particulares, ajenos al trabajo, aportando como prueba múltiples ficheros contenidos en el dossier «personal» que este empleado había creado en su ordenador.

En cuanto a las resoluciones judiciales a favor del derecho del empresario en los casos de despido por utilización inadecuada de Internet cabe destacar la Sentencia del Tribunal Superior de Justicia de Madrid de 16 de octubre de 1998 en la que se declara procedente el despido de un trabajador por utilizar Internet, conectándose a páginas de ocio, de compras, pornográficas, etc., además de utilizar el ordenador de la empresa para almacenar su correspondencia particular y el listado de precios confidencial de la empresa para utilizarlos en su negocio propio. Por su parte, la Sentencia del Tribunal Superior de Justicia de Murcia, de 15 de junio de 1999, declara procedente el despido de un trabajador que utilizó los servicios informáticos de la empresa para cuestiones particulares, poniendo en Internet una dirección de correo electrónico que correspondía al ordenador de la oficina comercial de la empresa. La Sen-

²⁸ *Boletín de Legislación*, Año VII, nº 288, Madrid, 21 de julio de 2003, Desayuno-Tertulia celebrado el mes de junio en la Escuela Judicial de Barcelona, sobre «El auge de la actividad delictiva de Internet».

tencia del Tribunal Superior de Justicia de Castilla y León (Valladolid), de 29 de enero de 2001, declara procedente el despido de una trabajadora que durante su jornada laboral y durante un dilatado período de tiempo había realizado conexiones a Internet para cuestiones ajenas a su actividad laboral, como visitar espacios de tiendas, tales como El Corte Inglés, Zara, Mango, y programas como El Bus y Gran Hermano. Por otra parte, la Sentencia del Tribunal Superior de Justicia de Madrid, de 4 de diciembre de 2001, declara procedente el despido de un trabajador que dedicaba su jornada laboral a descargar de Internet y visualizar una serie de ficheros de contenido pornográfico, utilizando su clave personal de acceso al ordenador. La Sentencia recalca que lo trascendente no es el contenido de los ficheros descargados sino la dedicación de la jornada laboral, en su totalidad, a actividades ajenas a las profesionales.

En el grupo de las resoluciones judiciales relativas a Internet a favor del derecho del trabajador destacaremos las siguientes. La Sentencia del Juzgado de lo Social nº 1, de 4 de abril de 2000, en la que se considera que como la empresa colocó en el ordenador del trabajador una aplicación informática que no podía ser detectada por el usuario y que se activaba de forma automática cada vez que se encendía el ordenador identificando todas las teclas pulsadas por el usuario, los programas activados y las ventanas del programa Windows, permitiéndose así el control del uso del ordenador por el empresario, la obtención de la prueba de utilización indebida del ordenador se realizó vulnerando el derecho a la intimidad del trabajador, pues se revelaba así la ludopatía del mismo. A través de este control del uso del ordenador se comprobó que de 35 días el trabajador se conectó 33 a un juego de cartas, durante un período medio de dos horas diarias. La Sentencia del Tribunal Superior de Justicia de Andalucía, de 25 de febrero de 2000, se declara que se lesiona el derecho a la intimidad del trabajador a través del registro realizado por la empresa en la terminal del ordenador sin que el trabajador esté presente y ante varios miembros del Comité de empresa y de la copia de dicha terminal de la carpeta denominada «mis documentos» y la carpeta denominada «Pepote». El artículo 18 del Estatuto del Trabajador admite el registro de los terminales del ordenador cuando sea necesario para proteger el patrimonio empresarial y el de los demás trabajadores, lo que no sucede en este caso resultando inválida la prueba así obtenida.

En cuanto a las resoluciones judiciales relativas al correo electrónico a favor del derecho del empresario cabe destacar la Sentencia del Tribunal Superior de Justicia de Cataluña, de 5 de julio de 2000, que declara procedente el despido de dos trabajadores por

transgresión de la buena fe contractual y abuso de confianza, por realizar actividades, como envío de correos electrónicos de contenido obsceno, totalmente ajenas a sus puestos de trabajo y por desobedecer las órdenes de la empresa de no utilizar los medios informáticos para uso particular. La Sentencia del Tribunal Superior de Justicia de Cataluña, de 14 de noviembre de 2000, declara procedente el despido de un trabajador por transgresión de la buena fe contractual. Este trabajador había enviado 140 correos electrónicos a 298 destinatarios en un mes y medio, a través de los ordenadores de la empresa, con mensajes humorísticos, sexistas e, incluso obscenos, ajenos a la prestación de servicios a pesar de que la empresa había establecido normas que prohibían expresamente el uso privado de la informática. La Sentencia del Juzgado de lo Social de Madrid, de 13 de octubre de 2000, confirmó la sanción de suspensión de empleo y sueldo impuesta a un trabajador, miembro del Comité de Empresa, por enviar un correo electrónico interno informando del resultado de las negociaciones del Convenio Colectivo. El fundamento de la confirmación de la sanción no es el uso del correo electrónico, sino el engaño al que recurrió el trabajador para enviar el correo. La Sentencia establece que los representantes sindicales y unitarios han de tener la posibilidad de utilizar medios que sirvan para informar a sus representados, pero ello no significa que el trabajador pueda utilizar el correo electrónico sin su permiso expreso.

Y por último nos referiremos a aquellas resoluciones judiciales relativas al correo electrónico y que han sido favorables al derecho del trabajador. La Sentencia del Tribunal Superior de Justicia de Madrid, de 12 de junio de 2001, califica como conducta grave, y no muy grave, la de un trabajador que envió a otro empleado de la misma entidad bancaria, destinado en Norteamérica, un correo electrónico de contenido pornográfico. En la Sentencia el Tribunal razonó que la conducta del trabajador no era acreedora de la sanción de despido, aunque sí de otra sanción menor al ser una falta grave tal como dispone el XVIII Convenio Colectivo de Banca al declarar como «perturbación del servicio sin justificación legal», la realización en el centro de trabajo de «cualquier actividad ajena al interés de la empresa». La Sentencia del Tribunal Superior de Justicia de Castilla y León (Valladolid), de 30 de septiembre de 2002, considera improcedente el despido de un trabajador que había aprovechado la ausencia de una compañera de trabajo para enviar desde su terminal de ordenador un correo electrónico a los representantes de la empresa en la República Checa y en Barcelona, con la finalidad de gastar una broma. En el correo advertía a los destinatarios que les trataban muy mal, que tenían problemas de comunicación, que

se acabaron las conversaciones hace una hora, etc. Tras dos horas mandó otro correo a dichos representantes de la empresa que eran amigos personales suyos advirtiéndoles que era una broma. La Sentencia razona que no es correcto ni serio este proceder del trabajador, pero tampoco ha de ser sancionado con el despido, ya que simplemente se trataba de gastar una broma a otros compañeros de trabajo y amigos, sin que trascendiera fuera de la empresa y siendo rectificada poco tiempo después.

En otros países las soluciones han sido las siguientes. En los Estados Unidos la legislación autoriza a los empresarios la vigilancia electrónica rutinaria. Asimismo, existen leyes de protección (*The Federal Wiretapping Act* y *Electronic Communications Privacy Act*) y legislación específica de cada Estado que impide la descripción de un marco legal único. En Gran Bretaña la *Regulation of Investigatory Powers Act* permite la apertura de correo electrónico, y la *Lawful Business Practice Regulations* autoriza a monitorear o grabar comunicaciones en múltiples supuestos. Por su parte la *Human Rights Act* establece el derecho a la privacidad. En Francia la justicia ha determinado que las cuentas de correo electrónico del trabajo están amparadas por el secreto. En Bélgica el tribunal de trabajo de Bruselas dictó una sentencia que establece el envío de correos electrónicos personales desde la empresa pertenece a la intimidad del trabajador y considera su número, tamaño y carácter privado como suficiente para una sanción sin necesidad de intervenir los mismos. Por último, en Japón la nueva ley de interceptación de comunicaciones permite el acceso a los correos electrónicos en el curso de una investigación de delitos graves como tráfico de drogas y armas o asesinatos.

IV. A MODO DE CONCLUSIÓN

Las intervenciones que se producen en la vida privada de las personas a través de las tecnologías son innumerables y aumentan día a día. A lo largo de estas páginas se ha intentado llamar la atención sobre los peligros que amenazan nuestra libertad. Sin embargo, no es nuestro objetivo transmitir un mensaje exclusivamente negativo, pues el progreso tecnológico conlleva avances y mejoras que pueden redundar en un incremento de la calidad de vida de las personas. En este sentido, cabe afirmar que el dato, la información y el conocimiento son eslabones de la misma cadena, o utilizando palabras de RIVERO LAGUNA «la cara y la cruz de la moneda de oro que tenemos en nuestras manos según se utilicen para generar riqueza añadida; o introducir abusos ilegítimos, el dato en sí mismo puede ser

irrelevante, no así su información asociada; y desde luego determinante el conocimiento que puede llegar a generar»²⁹.

La implantación de las tecnologías no resulta suficiente para alcanzar los logros que promete la Sociedad de la Información, pues el hombre es quien dirige las máquinas. Por tanto, sólo cuando las Políticas de Información incorporen el principio de la máxima efectividad de los derechos de la persona se conseguirá conciliar la tecnología y la libertad para que el desarrollo de la libre personalidad no quede supeditado a un determinismo tecnológico ni a intereses puramente económicos y comerciales. Sólo el respeto a la libertad y, por tanto, la existencia de un sólido compromiso democrático, harán posible que en este nuevo mundo informacional los individuos no se vean reducidos a una mera representación abstracta obtenida a partir del cruce o interrelación de datos.

El Derecho Constitucional, que regula la convivencia en el seno de la comunidad política, asume como tarea primordial la realización de la libertad e igualdad, así como el respeto de la dignidad y desarrollo de la personalidad. Partiendo de esta idea general y propiciado por la implantación de las nuevas tecnologías de la información y de la comunicación, se ha ido desarrollando un nuevo derecho fundamental, el llamado Derecho a la Autodeterminación Informativa o de Protección de Datos, que permite que sean las personas quienes decidan sobre su propia vida al erigirse el principio del consentimiento como eje de su contenido. Este derecho, reconocido y protegido tanto a nivel interno de los Estados como a nivel internacional, garantiza que, perteneciendo los datos relativos a la persona al ámbito de su vida privada, corresponde al interesado decidir sobre la posibilidad, mayor o menor, de que sean conocidos por terceras personas y, en todo caso, sobre el control o disposición de los mismos.

²⁹ LAGUNA RIVERO, J.: «Prólogo» a DEL PESO, E.: *Ley de Protección de Datos. La nueva LORTAD*, Madrid, 2000, pág.XXVI.