UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO
Departamento de Derecho Constitucional

TESIS DOCTORAL

Protección de datos y seguridad de Estado

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Ofelia Tejerina Rodríguez

Directores

José Luis Piñar Mañas
Ignacio Torres Muro

Madrid, 2012

PROYECTO DE TESIS DOCTORAL

PROTECCIÓN DE DATOS
Y
SEGURIDAD DE ESTADO

OFELIA TEJERINA RODRÍGUEZ

DEPARTAMENTO DE DERECHO CONSTITUCIONAL
ESTUDIOS SUPERIORES DE DERECHO CONSTITUCIONAL
UNIVERSIDAD COMPLUTENSE DE MADRID

DIRECTORES:

D. JOSE LUIS PIÑAR MAÑAS y D. IGNACIO TORRES MURO

"Pues quién negará que se elevó su corazón, y que en su pecho, más libre latió la sangre con más pureza cuando se elevó el primer fulgor del nuevo sol, cuando se oyó hablar de los derechos del hombre, comunes para todos, de la libertad embriagadora y de la hermosa igualdad."

W. Goethe, "Hermán y Dorotea" 1.796

INDICE

INTRODUCCIÓN

El permanente desarrollo tecnológico de la sociedad ha supuesto un replanteamiento del sistema de derechos fundamentales en los países desarrollados, su vigencia en cada momento, ha llevado a implantar diferentes mecanismos de amparo para las potenciales amenazas que se supone van a surgir. En este periodo concreto de diseño de la "Sociedad de la Información", las tecnologías de la información y de las comunicaciones están influyendo de manera decisiva sobre los llamados "derechos civiles o de primera generación"[1], pues han propiciado la aparición de nuevos planteamientos de los Principios y Normas Fundamentales de cada grupo humano, en cada momento y lugar, y en función de las necesidades que requieren cubrir.

Esta influencia se puede descubrir de forma muy precisa partiendo de una teoría de corte evolucionista y respecto de un ejemplo especial, el que muestra el artículo 18.4 de la Constitución Española. La Constitución recoge en ese precepto una garantía concreta, para un derecho fundamental concreto, que se ha ido forjando "en" la Sociedad de la

[1] Denominación que reciben los derechos fundamentales que hacen referencia al ámbito de autonomía de la persona humana y de los grupos sociales en relación a la actuación de los órganos del Estado.

Información: es el derecho a la protección de datos personales[2]. La comprensión del desarrollo de este derecho ha sido conflictiva desde que se sugirió la identidad del ser humano, y el derecho a preservarla, como parte de su dignidad. Aunque la doctrina mayoritaria comparte la idea de un origen similar al que mostró la evolución del resto de los derechos fundamentales (respetando "el tiempo de los derechos"), no siempre ha sido así, incluso hoy se defiende su aparición "ex novo" para este momento sociológico[3].

La tesis de la evolución lógica y ordenada del derecho a la protección de datos, de conformidad con la evolución del entorno en que se mueve el individuo, requiere entender en primer lugar las diferencias teóricas del conflicto jurisprudencial y doctrinal en la determinación del origen de este derecho. Se distingue pues entre aquellas que propugnan su creación como un nuevo derecho fundamental y, las que defienden la "ampliación" de derechos fundamentales preexistentes, ambas dirigidas siempre sobre el concreto derecho a la protección de las personas ante el uso de la informática. El sector de la doctrina[4] que considera su aparición "ex novo", basa sus conclusiones en la previsión formal de este derecho en las Constituciones vigentes y, su confirmación, a través de la jurisprudencia o de las denominaciones de que le iba dotando el Alto Tribunal ("Libertad Informática", "Derecho de autodeterminación informativa" o "Derecho a la Intimidad Informática"). Sitúan este derecho entre los llamados "derechos de tercera generación". El sector doctrinal opuesto[5] alega sin embargo, que

[2] Artículo 18.4 CE: "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

[3] "El artículo 18.4 de la CE incorpora una garantía constitucional, para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona". STC 254/93.

[4] MORALES PRATS, F.: "Protección penal de la intimidad, frente al uso ilícito de la informática en el código penal de 1995". Delitos contra la libertad y Seguridad. Cuadernos de Derecho Judicial. Escuela Judicial. CGPJ. Madrid, 1996. pp. 147 – 196; BAON RAMIREZ., R. "Visión general de la informática en el nuevo Código Penal. Ámbito jurídico de las tecnologías de la información *Revista del Consejo General del Poder Judicial*. C.G.P.J. Madrid, 1996. pp. 82 - 85; GONZÁLEZ QUINZÁ, A. "Comentario a la STC 254/1993, algunas consideraciones en torno al artículo 18.4 CE y la protección de los Datos Personales", *Informática y derecho: Revista iberoamericana de derecho informático*, Nº 6-7. Madrid, 1994. pp. 203-248; FAIREN GUILLEN, V. "El Habeas Data y su protección actual surgida en la Ley española de informática de Informática de 29 de octubre de 1992. *Revista de Derecho Procesal*. Ed. de Derecho Reunidas S.A. Madrid, 1996. pp. 523 - 527.

[5] GONZÁLEZ MURÚA, A.N., "Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de datos", *Revista Vasca de Administración Pública*, Nº 37. 1993. pp. 227-270; LÓPEZ DIAZ, E., *El Derecho al Honor y el Derecho a la Intimidad: Jurisprudencia y Doctrina.* Ed. Dykinson. Madrid, 1996; ORTI VALLEJO, A. *El derecho a la intimidad e informática*. Ed. Comares. Madrid, 1994; VILLAVERDE MENÉNDEZ, I. "Protección de datos personales, derecho a ser informado, y autodeterminación informativa del individuo. A propósito de la STC 254/1993". *Revista*

los valores fundamentales de la existencia humana cobran un sentido diferente en función de las circunstancias y el momento en que sean analizados, para así ir dotándolos de las garantías precisas que aseguren su efectivo ejercicio y, que sólo resultará posible reconocer y asimilar jurídicamente cuando se vean real o potencialmente amenazados.

Sobre lo que no existe discusión es que ambas líneas teóricas tienen un objetivo común para el artículo 18.4 de la CE, manifestar su contenido como la tutela de un derecho que lo requiere desde el momento en que se va a someter a tratamiento informatizado datos de carácter personal. Hoy es frecuente oír hablar de ello como "autodeterminación informativa[6]" "libertad informática" o "protección de datos".

Una vez comprendido que la razón de ser de este precepto constitucional son los "derechos de libertad" (derechos que ponen límite a las posibilidades de interferir en libertad del ser humano), y que su evolución debe continuar sobre la protección de la esfera libre del ser humano, para evitar ser desvirtuado por completo (en una tercera e incluso cuarta generación de derechos), es necesario analizar las razones que exigen preservar su contenido en la Sociedad de la Información, y sobre todo ante determinadas amenazas. En cualquier caso, este contenido habrá de ser analizado siempre en relación con la salvaguarda de otros intereses superiores, derechos y libertades que podían verse afectados de manera colateral si se produce la "mutilación" de esta "libertad informática"[7].

La Constitución española es la norma que establece los derechos que deben ser considerados fundamentales para los individuos y, para su

---

Española de Derecho Constitucional, Nº 41. Madrid. Mayo – Agosto, 1994. pp. 187 – 224; LUCAS MURILLO DE LA CUEVA, P. "Diez preguntas sobre el derecho a la autodeterminación informativa y la protección de datos de carácter personal". Conferencia que tuvo lugar el día 24 de octubre de 2005 en la sede de la Agencia Catalana de Protección de Datos: ·Sin embargo, es importante advertir que no es éste un caso de creación ex novo de un derecho fundamental. Se trata, más bien, de un supuesto de invención o hallazgo --en el sentido de la inventio romana-- de este derecho en el artículo 18.4 de la Constitución. Y, también, de construcción de su régimen jurídico" (…). Disponible en: http://www.apd.cat/media/305.pdf

[6] *(...)* "el derecho que asiste a una persona para decidir, por sí misma, de qué datos pueden disponer otros y en qué circunstancias, con qué límites, pueden ser revelados en cuando forman parte de su intimidad (son secretos de su vida)". BAÓN RAMÍREZ, R. Visión General de la Informática en el nuevo Código Penal. *Revista del Consejo General del Poder Judicial*. Núm. XI. Ámbito jurídico de las tecnologías de la información. Madrid, 1996. p. 82.

[7] Entendido este concepto en el contexto de la "protección de datos de carácter personal".

garantía o efectivo ejercicio, sistematiza igualmente la organización y actuación de los poderes públicos para su respeto y defensa.

Esta ilustre finalidad no siempre es cumplida con la mesura y proporcionalidad que pretende, en ocasiones, su aplicación se puede ver seriamente dificultada por la necesidad de armonizar otros intereses propios de la convivencia de los individuos en sociedad. La función del Estado respecto de este objetivo es la de proporcionar armonía en el ejercicio del conjunto de derechos fundamentales, debe en todo caso, conseguir la realización de todos ellos evitando que sea cercenado su contenido esencial o desvirtuada su razón de ser.

En este sentido, y siguiendo la evolución del citado artículo 18.4 de la Constitución, es importante mostrar que uno de los intereses o derechos que con mayor intensidad se está viendo limitado por los últimos acontecimientos histórico – sociales, es efectivamente el derecho a la protección de datos de carácter personal, y en concreto, en materia de terrorismo y Seguridad de Estado, pues éste es considerado el "interés general superior" en toda su amplitud.

Cuando el Estado quiera limitar el ejercicio de un derecho fundamental para proteger otro, podrá hacerlo siempre y cuando tenga en cuenta la proporcionalidad en las medidas tomadas y las finalidades perseguidas. Este principio básico de las sociedades democráticas no siempre es respetado, y bajo el manto de la "Seguridad del Estado" se incumplen los cometidos que encomienda la Constitución, los diferentes Tratados, Cartas y demás normativas existentes sobre Derechos Humanos que exigen que internacionalmente sea respetada la dignidad del individuo.

En concreto, el tema que se aborda en este trabajo intenta mostrar que una primera fase de control estatal pasa por invadir una parte muy importante de la esfera decisora del individuo, la que afecta a su propia información personal. Este es el elemento más atractivo, y más vulnerable a la vez, del individuo, en el sentido de lo sencillísimo que resulta intervenirlo y la excepcional capacidad fiscalización que ofrece a quienes

poseen dicha información. Por este motivo, y para evitar invasiones innecesarias en la esfera decisora de cada sujeto, es preciso determinar con cautela qué es efectivamente la realización de intereses superiores o generales más importantes.

En definitiva, para comprender el sentido de esta tesis, se analizan distintas fases y elementos de un derecho fundamental autónomo[8], y se expone sobre todo cómo afecta al individuo y por qué es necesario proteger el ejercicio de su contenido esencial, a pesar de la evolución histórica y social en su requerimiento de amparo.

[8] STC 292/2000 (F.Jº. 6º): "el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno", mientras que el derecho a la protección de datos "garantiza a los individuos un poder de disposición sobre esos datos".

I. PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES.

1.- Evolución.

La definición teórica de LUIGI FERRAJOLI[1] plantea para esclarecer el concepto "derecho fundamental", se ha querido tomar como referencia porque expone todos los elementos que deberían conformar su contenido esencial: derecho subjetivo; que corresponde a las personas; previsto en su ejercicio por una norma jurídica y, con carácter universal. Hablamos de una expectativa o necesidad (positiva o negativa) que corresponde siempre a un sujeto por su condición de persona, por mediación de una norma (no necesariamente escrita) y con un carácter inalienable e indisponible. Cuestión distinta es la visión que se quiera dar de cada uno de estos elementos, que por razones de extensión no será objeto de este trabajo

[1] "Son "derechos fundamentales" todos aquellos derechos subjetivos que corresponden universalmente a "todos" los seres humanos en cuanto dotados del status de personas, de ciudadanos o personas con capacidad de obrar; entendiendo por "derecho subjetivo" cualquier expectativa positiva (de prestaciones) o negativa (de no sufrir lesiones) adscrita a un sujeto por una norma jurídica; y por "status" la condición de un sujeto, prevista asimismo por una norma jurídica positiva, como presupuesto de su idoneidad para ser titular de situaciones jurídicas y/o autor de los actos que son ejercicio de éstas". FERRAJOLI, L. *Los Fundamentos de los Derechos Fundamentales*. Ed. Trotta. Madrid, 2001. p.19.

más que en aquello en que se aproxime a las "teorías realistas", su distinción de otras, y en particular, su aproximación a la esencia del derecho a la protección de datos. Es importante que, antes de abordar las implicaciones humanas de este específico derecho respecto de la política estatal en materia de seguridad y terrorismo, se citen algunas consideraciones sobre lo que conlleva el significado del concepto "derecho fundamental". También será de gran utilidad para el posterior desarrollo de este estudio, entender desde un principio cómo se comporta su núcleo esencial ante situaciones de constante desarrollo, pues nos permitirá entender también la evolución de sus garantías en ejercicio.

Como punto de partida se ha de considerar que la corriente filosófica que apuesta por el realismo, configurado el entre el iusnaturalismo y el iuspositivismo, ajusta en este contexto la tesis de que los derechos fundamentales no son ideales atemporales en sí, ni se mantienen estáticos en un plano teórico, sino que son el producto de exigencias del momento social que vive el individuo que los reconoce y, a quien van dirigidos[2]. Además plantea que, si carecen de garantías que permitan su ejercicio, es que en realidad no existen. De alguna manera las teorías realistas, prevén la necesidad de protección del ejercicio del derecho por una norma para poder comprender y asimilar que como seres humanos, los derechos nos pertenecen. Insisten también en la necesidad de un marco político y legal adecuado para el disfrute efectivo de los derechos fundamentales, y así se justificará más adelante al hablar de la articulación del conjunto de derechos y sus límites.

Pongamos pues que dicho sistema organizado se da para la puesta en práctica de un derecho fundamental, que existe su reconocimiento en la sociedad y, que tiene una garantía que permite su realización efectiva. Este marco así esbozado, nos permitirá considerar la idea básica de que los derechos deben ser protegidos y sus garantías evolucionar, de tal forma que, una definición como la que da HELMUT COING para los derechos fundamentales, que explica que son "los derechos subjetivos directamente

[2] PÉREZ LUÑO, A. *Derechos Humanos, Estado de Derecho y Constitución*. Ed. Tecnos. Madrid, 1999. p. 59.

relacionados con las facultades de autodeterminación del individuo"[3]. Esta autodeterminación es la que plantea el hecho de que para la verdadera eficacia del derecho fundamental, las garantías de su ejercicio deben dirigirse en todo caso hacia la realización de la esencia humana. Este es el núcleo, la verdadera razón de ser de los derechos fundamentales. Ahora bien, la forma de manifestarse (tanto del derecho como de sus garantías) dependerá en todo caso del momento histórico, social y político que analicemos, y generalmente lo será en función de las amenazas que los hagan peligrar. Se integra por tanto "el tiempo de los derechos" como elemento imprescindible en su configuración práctica, tal y como explicaba CÁMARA VILLAR al reconocer que "está en la naturaleza de los derechos, en cuanto realidades históricas, encontrarse permanentemente "in fieri", prendidos de las exigencias morales de la sociedad de cada tiempo y, sujetos a la mayor o menor sensibilidad que los legisladores tengan respecto a los problemas básicos de la convivencia humana"[4].

Este planteamiento (núcleo esencial, garantías, marco social) nos lleva a mostrar que las condiciones definitorias del hombre son muy concretas y, su efectiva realización, debe darse independientemente de las amenazas que se le planteen en un momento dado, por eso, se trata de ver la reacción de estas condiciones en relación con el progreso de sus expectativas en cada momento.

Aunque las posturas realistas puras en general, resuelven el problema de la fundamentación de los derechos humanos entendiendo que "existe una convicción generalmente compartida de que ya están fundados, que hay un consenso general sobre su validez" [5], a los efectos de esta exposición sólo se puede entender dicho consenso respecto de las condiciones o necesidades básicas del hombre: supervivencia e integridad física, libertad, e igualdad, en definitiva la "autodeterminación" de COING;

[3] CASTÁN TOBEÑAS, J. Cita a H. COING en su obra *Los derechos del Hombre*. Ed. Tecnos. Madrid, 1968. p. 24.
[4] BALAGUER CALLEJON, F. (Coord.) y otros. *Manual de Derecho Constitucional*. Vol.II. "Derechos y libertades fundamentales deberes constitucionales y principios rectores instituciones y órganos constitucionales". Ed. Tecnos. Madrid, 1999. p.45.
[5] BOBBIO, N. "Presente y porvenir de los derechos humanos". *Anuario de los Derechos Humanos*, Nº 2 (Enero). Madrid, 1982. pp. 10 y 45.

sobre esto, habrá que considerar el momento histórico, social y político que, a través del "pactum libertatis", determinará cómo se han de proteger y garantizar, dichas bases para su efectiva realización.

NORBERTO BOBBIO, explica aquella "autodeterminación" en este sentido, diciendo que el fundamento de los derechos está en la necesidad del hombre, toda necesidad supone una carencia, el hombre tiene necesidades en cuanto carece de determinados bienes y siente la exigencia de satisfacer esas carencias[6]. También para BOBBIO, la satisfacción de las necesidades humanas (necesidad de vivir en un marco de dignidad, igualdad y libertad que permita un desarrollo integral de su personalidad) es lo fundamental, y a partir de su análisis, lo será también el cómo protegerlo. BENTHAM, por su parte, coincidía con estos planteamientos pero centraba la cuestión señalando que "las buenas razones para desear que existan los derechos del hombre no son derechos, las necesidades no son los remedios, el hambre no es el pan"[7], y es cierto, las necesidades no son los derechos, pero sí lo que los va a enfocar o alumbrar. Lo que se pretende al citar estas tesis es mostrar que no son las necesidades (se entiende las primarias) del hombre las que cambian, sino que debe hacerlo la forma de proteger su efectiva satisfacción: las garantías son las que deben evolucionar. Siguiendo a BENTHAM, el hambre sería la necesidad y el pan el derecho a satisfacerlo (el derecho fundamental). Se puede pues afirmar que un "derecho fundamental" que ya existe, será conceptuado y dotado de contenido cuando la amenaza se haga patente y se de por tanto la necesidad de protegerlo. No habría lugar para una aparición "ex novo", y así se planteará para el específico derecho a la protección de datos personales.

FERRAJOLLI y BOBBIO, aunque distintos en sus planteamientos, parten de un interesante lugar común para una solución ecléctica, que es la

[6] BOBBIO, N. *Teoría General del Derecho*. Ed. Debate. Madrid, 1991. BOBBIO señala respecto de la composición del ordenamiento jurídico que "se entiende por "laguna" también la ausencia no ya de una solución cualquiera que ésta sea, sino de una solución satisfactoria o, en otras palabras, no ya de la ausencia de una norma, sino la falta de una norma justa, o sea, de aquella norma que se desearía existiese y que no existiese" (p. 238), es decir, sostiene, que la "necesidad" es una fuente del derecho (p. 264).

[7] "But reasons for wishing there were such things as rights, are not rights; - a reason for wishing that a certain right were established, is not that right - want is not supply - hunger is not bread". BENTHAM, J. *Anarchical Fallacies,* Works Vol. 2, Ed. Bowring, Edinburgh, 1843. Se puede consultar el texto completo en: http://www.ditext.com/bentham/bentham.html [2005, 21 de abril].

que se considera como la más adecuada. El primero establecía una fundamentación objetivista, de validez absoluta o universal con independencia de la experiencia de los individuos o de su consciencia valorativa, pero el segundo, centraba su esencia en un tiempo concreto y, en función de cómo avanzase éste, dicha esencia iría mutando, lo que nos exige forzosamente un análisis "empírico", basado en la razón del momento y en la autonomía humana como fuente de todos los valores.

¿Qué es entonces lo que condiciona la existencia, la vigencia y, en definitiva, la eficacia real derecho fundamental? ¿Es el tiempo en que se contempla? ¿Es su esencia atemporal? Se quiere poner de manifiesto que son ambos elementos los que configuran la validez del derecho, que para entender su sentido siempre debemos tener presente cómo se adaptan sus garantías al tiempo y, como se ha venido diciendo y se corroborará después, que las "necesidades de protección" de sus destinatarios se materializarán según el momento social, político o económico en que se desarrolle el individuo en cuestión. Es imprescindible poner en conexión directa al ser humano con aquello que amenaza su condición (ser humano – necesidad – amenaza – protección), y debe hacerse en cada época, cambian las amenazas y por ello las necesidades de protección[8]. Se puede afirmar que el "derecho" existe siempre porque las necesidades básicas de un ser humano son en esencia las mismas, tal y como propugnan las teorías objetivistas y, siguiendo teorías subjetivistas, que la forma de garantizarlo es la que cambia, pues se materializa en función del momento que lo contemple y lo exija (son las necesidades de protección las que cambian).

Estos planteamientos "cuasi-filosóficos" tiene fiel reflejo en el ejemplo que se anunciaba protagonista de este estudio: el artículo 18.4 de la Constitución Española. Dicho artículo establece que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

[8] "La noción de necesidad que lleva al reconocimiento del derecho suele implicar además, la negación de la posibilidad de satisfacerla de modo libre y espontáneo". LUCAS MURILLO DE LA CUEVA, P. Ponencia *Avances Tecnológicos y Derechos Fundamentales. Los riesgos del Progreso*. "Derechos Humanos y Nuevas Tecnologías", XIV Curso de Verano UPV. Col. "Jornadas sobre Derechos Humanos", Nº 6. San Sebastián, 2002. p. 38.

En este precepto se observa claramente cómo el desarrollo social y de la tecnología en el tiempo, pueden determinar la definición de lo que "debe ser" inherente a la persona por el simple hecho de serlo. En el caso del artículo 18.4 de la Constitución, "debe ser" el desarrollo de sus libertades frente a la informática, formulando aquello que le va a permitir vivir en un marco de dignidad, igualdad y libertad, frente a la tecnología y, al fin y al cabo, todo ello se debe traducir en un efectivo desarrollo integral de su personalidad.

Hoy los cambios se suceden a un ritmo vertiginoso, los modos y medios de vida se ven seriamente afectados en todos y cada uno de sus aspectos principales, de manera que el impacto tecnológico no sólo está marcando las relaciones entre los individuos, sino que también está incrementando las diferencias entre ellos (sus "necesidades de protección" son distintas). Es obvio que un individuo que vive totalmente fuera del alcance de las aplicaciones y utilidades de determinada tecnología, no verá nunca amenazada ni reducida por ésta su esfera de dignidad, pero en la medida que el desarrollo de la tecnología se da para todos, el hecho de no tener acceso a ella, no implica necesariamente verse al margen de sus beneficios o perjuicios. Sin embargo, si significa que el ser humano va a priorizar sus preferencias a la hora de exigir determinadas garantías frente a concretas amenazas, dependiendo del "estado de necesidad" en que se encuentre demandará uno u otro sistema de protección específico (por ejemplo, si su integridad física está en peligro, no se planteará como prioridad, mantener su intimidad lejos de "ojos ajenos" o exigir que le dejen expresarse con libertad).

Los valores y las prioridades que imperan en cada sociedad están en función de las circunstancias reales que en ella se viven, y así también lo estará el contenido de los derechos fundamentales en su aplicación real o práctica, en sus garantías. La libertad era y es lo mismo independientemente de la sociedad en que se viva, pero es en función de las amenazas existentes en cada momento, cuando habrá que plantearse dotarla de uno u otro contenido práctico (de una garantía concreta) y esto, es lo que hace en definitiva el artículo 18.4 de la Constitución española, prevé que la libertad,

en este caso sobre la capacidad decisora individual, se puede ver amenazada por un peligro concreto y lo protege con la Norma.

2.- Garantías.

En el apartado anterior hemos establecido que los derechos en general, y en concreto los "fundamentales", no surgen de manera espontánea ni previa a las necesidades a que suelen dar respuesta, si no que su configuración se debe a un complejo proceso de evolución (necesidad básica que se ve amenazada, y para ella surgen nuevas "necesidades de protección", porque existe "de facto" el derecho a ver satisfechas ambas necesidades)[9]. Sobre esto se ha de reconocer el planteamiento que propone que, sin garantías de efectiva realización en la práctica, van a tener my poco sentido y, por tanto, es imprescindible su determinación y promover su respeto de forma general.

Simplemente examinando su denominación, vemos que las Constituciones los registran como "derechos fundamentales" y los Tratados Internacionales (bajo la inspiración de las revoluciones francesas y sus "derechos del hombre") como "derechos humanos". Estas diferencias, son consecuencia del progreso sobre la forma de valorar la importancia y alcance de estas figuras, respecto de la dignidad de aquellos a quienes se pretendía protegieran: el ciudadano en concreto y la persona (o el ser humano) en general. Muchas son las voces que sientan el origen de los derechos humanos sobre reivindicaciones de cuotas de "poder" social por las clases dominadas[10], pero también se han tratado como sencillas normas de convivencia, destinadas a organizar a los ciudadanos en el respeto mutuo[11].

---

[9] "Derechos humanos son el conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional". PÉREZ LUÑO, A. *Derechos Humanos, Estado de Derecho*..., Op. Cit. p. 48.

[10] Textos como el código que el dios Samash (dios Sol o dios de la Justicia) entrega al rey Hammurabi, el "Código de Hammurabi", (Siglo XVIII a.c., Imperio Babilónico), que fue promulgado con el objetivo: "de humillar a los malos e injustos e impedir que el poderoso perjudique al débil; para que toda persona

En Europa, la "Petition of Right" y el "Bill of Rights" ingleses de principios y finales del siglo XVII respectivamente, plasmaron una idea más global de lo que debe ser considerado "derecho humano", nos dan una idea de qué es lo que debe estar reconocido y la calidad de dicha consideración. Estos textos sirvieron de ejemplo para otros posteriores, como los que resultaron de las revoluciones norteamericanas y francesas del siglo XVIII: la Declaración de Independencia Norteamericana, la Declaración de Derechos de Virginia de 1776 y la Declaración Francesa de los Derechos del Hombre y del Ciudadano en el año 1789. Esta última recogió un importantísimo conjunto de principios enunciados en tan sólo 17 artículos, que hoy son considerados esenciales para todas las sociedades humanas por ser ejemplo y compendio de las principales necesidades humanas a cubrir y proteger.

Esta breve mención de lo histórico, hasta la promulgación de las primeras declaraciones de derechos humanos, descubre cómo las sociedades varían en función de las amenazas a su estabilidad, cómo en todos esos momentos de la historia los cambios se van materializando en exigencias de seguridad, de protección o de dignidad para las personas que las componen, personas que precisamente han sido artífices de esas revoluciones para lograr esos cambios. Así se forman y, consolidarán las garantías para la estabilidad.

La Declaración francesa de los Derechos del Hombre y del Ciudadano de 26 de agosto de 1789, consolida un importante proceso de desarrollo en este sentido, pues es promulgada como garantía material de reconocimiento de derechos. El siguiente artículo es un buen ejemplo del contexto que se ha descrito hasta aquí:

---

perjudicada pueda leer las leyes y encontrar justicia". Disponible en: VÁZQUEZ HOYS, A.M. http://www.uned.es/geo-1-historia-antigua-universal/SUMERIOS/sumerios7%20_hammurabi.htm [2005, 22 de abril].

[11] En el derecho romano, se legislaba para el ciudadano. Sólo éste podía participar en la vida política de la ciudad como miembro de un grupo que debía respetar las normas que ordenaban la convivencia, normas que aparecían estrictamente positivizadas. Al aludir a este sistema de Derecho se quiere hacer una llamada sobre la idea de que la evolución de la sociedad ha hecho evolucionar a su vez lo que en su día fue sustrato de configuración para los derechos humanos, así una de las grandes aportaciones de este periodo fue la apertura de la protección que había implicado el término "ciudadano" a un número cada vez mayor de personas, ricos y pobres, de una u otra clase, determinando que todos los hombres son ciudadanos de un estado universal. Esta comunidad universal era fruto de la crisis de la "polis" y decía Marco Aurelio que: "Por ser Antonio, mi patria es Roma; pero por ser hombre, mi patria es el mundo", lo que determina su alcance sobre el humano y no tanto sobre las fronteras geográficas o políticas.

> Artículo 2º - "El fin de toda asociación política es el mantenimiento de los derechos naturales e imprescriptibles del hombre. Estos derechos son la libertad, la propiedad, la seguridad y la resistencia a la opresión".

Se puede observar en él que garantizar un derecho como la "asociación política" se hace con un objetivo concreto: amparar y garantizar otros derechos humanos afines.

Ya en el Siglo XVIII, comienzan a aparecer las constituciones de carácter liberal que quieren proteger los Derechos civiles y políticos, es decir, las libertades de vida y de propiedad del individuo, frente a la sociedad (no tanto "en la sociedad"). Con las revoluciones burguesas se configuran y consolidan los "Derechos de Primera Generación" o "Derechos civiles y políticos" como algo destinado a ser real y efectivamente aplicable, para decir al monarca que el Estado debe respetar siempre la vida, la integridad física y moral, la libertad personal, la seguridad personal, la igualdad ante la ley, la libertad de pensamiento, expresión y de opinión, de movimiento, de resistencia y de inviolabilidad del domicilio, etc. En definitiva se protege al hombre frente a Estado.

En el S.XIX las revoluciones industriales y luchas sociales dan paso a los llamados "Derechos de Segunda Generación", que son específicamente "Derechos sociales y económicos". La declaración de estos derechos, su afianzamiento, pretendía realizar la esperanza de los hombres de mejorar sus condiciones de vida (ya dentro de la sociedad), en lo económico y en lo cultural, exigiendo nuevas respuestas a nuevas formas de amenaza que se cernían sobre su estabilidad. Vemos por tanto como el catálogo de derechos existente se iba ampliando y se iba configurando para el respeto[12] en función de los movimientos reivindicativos de la época.

Los Derechos Humanos se van consolidando en el Siglo XX, a partir de la Segunda Guerra Mundial y, fueron acomodados en documentos escritos

[12] Las Constituciones de México de 1917, y la de Alemania de Weimar en 1919 son las primeras que comienza a plasmar estas ideas, y es a partir de este momento cuando se inicia el periodo más fructífero del reconocimiento internacional de derechos humanos como principios básicos de convivencia.

para ser respetados, porque esto facilitaba su percepción como vigentes y protegibles. Son ejemplos notorios y de obligada cita la Declaración Universal de Derechos Humanos, aprobada por las Naciones Unidas el 10 de diciembre de 1948 y el Pacto Internacional de Derechos Económicos, Sociales y Culturales, de 1966. Los derechos de "Segunda Generación" que recogen, cumplían con la necesidad del individuo de organizarse "en la sociedad" y, frente a aquello que pudiera ponerla en peligro, así se reconocen como tales: el derecho a la propiedad (individual y colectiva), a la seguridad económica, al trabajo (a un salario justo y equitativo, al descanso, a sindicalizarse, a la huelga), a la seguridad social, a la salud, a la vivienda, a la educación, etc.

Por último, ejemplificando la referida consolidación, hay que fijarse en la "Tercera Generación" de derechos (ya se empiezan a conocer como "derechos humanos"), que ya se empiezan a conocer como los "Derechos de los pueblos o de solidaridad". Se trataba del derecho a la paz, al desarrollo económico, a la autodeterminación, a un ambiente sano, a la solidaridad, etc., que se presentan como respuesta a lo que se llamó "liberties pollution"[13].

Hoy se han fijado y reconocido aquellos derechos que se creyó necesario garantizar por los cambios específicos que se estaban produciendo en la sociedad, en la forma de convivir de los individuos. Las necesidades sobre los diversos aspectos de la vida humana crecen y se intensifican, se demanda una mejor calidad por esos cambios en las circunstancias. Como nueva generación, no significa que sea una generación distinta de la anterior sino que "en cierto modo es también la anterior, porque necesariamente ha debido tenerla en cuenta para completar sus insuficiencias y corregir sus errores. De esta forma evolucionan los derechos humanos en dirección al

[13] "Contaminación de las libertades": término con el que algunos sectores de la teoría social anglosajona aluden a la degradación de los derechos fundamentales ante determinados usos de las nuevas tecnologías, y a la existencia en los últimos años, junto a la constatación y reivindicación de los tradicionales derechos (civiles y políticos y económicos sociales y culturales) de unas circunstancias que responden ante todo al valor solidaridad. "Los "derechos de la tercera generación" surgen como respuesta al fenómeno de la denominada "contaminación de las libertades" ("liberties pollution") y encuentran el marco espacial y temporal de su progresivo reconocimiento en el "Estado constitucional", que representa la tercera generación de Estados de Derecho, precedido del Estado Liberal -marco del reconocimiento de los derechos y libertades individuales- y del Estado Social -que contextualiza la consagración de los derechos económicos, sociales y culturales-". PÉREZ LUÑO, A. "Estado constitucional y derechos de la tercera generación". *Anuario de Filosofía del Derecho*, Vol. XIV. Valencia, 1997. pp. 563 y ss.

presente, acumulando el pasado en integrándolo con cada innovación. La historia de los derechos humanos se revela a la vez como paradigma y como progreso constante"[14].

En España, la Constitución de 1978, documento base del reconocimiento actual, consolidación y garantía de derechos, estableció también diferencias entre las necesidades que se consideró fundamental proteger. En el capítulo cuarto, "de las garantías de las libertades y derechos fundamentales", se señalan tres grandes bloques que reflejan las generaciones antes descritas y, cual es el criterio que considera para su protección[15]. Distingue entre: los derechos y libertades reconocidos en el capítulo segundo, los principios reconocidos en el capítulo tercero, y las libertades y derechos reconocidos en el artículo 14 y la sección primera del capítulo segundo. Es para estos últimos para los que otorga la máxima protección al decir en el artículo 53 que "cualquier ciudadano podrá recabar la tutela (...) ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional". En especial este recurso de amparo, supone una garantía añadida en la consolidación y el efectivo ejercicio de los derechos, va a tratar de garantizar su contenido esencial. El Tribunal Constitucional debe reponer en su situación original (antes de producirse la indefensión y siempre en lo posible) tanto al perjudicado como el propio orden constitucional vulnerado. A través de su interpretación de la CE, este organismo va a ir creando además, como instrumento de garantía añadido, una doctrina legal vinculante y preceptiva para los poderes públicos. Establece la STC 1/81, de 26 de enero, "la finalidad esencial del recurso de amparo es la protección de los derechos y libertades (...) cuando las vías ordinarias han resultado insatisfactorias (...)". Esta función interpretativa va

[14] PÉREZ LUÑO, A. *Derechos Humanos, Estado de Derecho...* Op. Cit. p. 48.

[15] Artículo 53 CE:

"1. Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161, 1, a).

2. Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30.

3. El reconocimiento, el respeto y la protección de los principios reconocidos en el Capítulo tercero informarán la legislación positiva, la práctica judicial y la actuación de los poderes públicos. Sólo podrán ser alegados ante la Jurisdicción ordinaria de acuerdo con lo que dispongan las leyes que los desarrollen".

a permitir que la CE, principal fuente de protección, pueda seguir el ritmo del desarrollo y progreso social de manera suficientemente flexible como para evitar el estancamiento de su texto escrito.

La importancia de la doctrina constitucional en la afirmación de los derechos, reveladora en la aplicación de garantías, es parte del objeto de este estudio y se va a ir desgranando en sucesivos capítulos, respecto del específico derecho a la protección de datos de carácter personal, por ser ejemplo destacado y protagonista de una situación de avanzado desarrollo social en el sentido más tecnológico, y por constituir un derecho fundamental ha necesitado ser garantizado para poder consolidarse como efectivo. Tenemos por tanto el derecho, la evolución social y la garantía, nos queda por analizar los límites para su ejercicio.

Pero antes de centrarnos en el estudio del elemento "integrador", o de realización material, de la configuración de los derechos, esos límites en la articulación de su ejercicio, para todos y cada uno de los integrantes de la comunidad (en especial, en el entorno legal y político), es muy importante citar aquí otro instrumento de consolidación: la educación de los destinatarios de los derechos.

El aspecto educativo en los destinatarios, es un componente más en la configuración de un entorno positivo para el ejercicio de derechos, pero debe ser tenido en cuenta, por sus efectos al considerar los derechos fundamentales como específicos de una sociedad determinada. Formar individuos en derechos humanos es un reto que no siempre se materializa como debiera, de tal forma que, inevitablemente, muchos de ellos se quedan al margen de los efectos de su contenido esencial. Así, nos encontramos en la práctica con el problema de quiénes se ocuparán de fomentar el respeto a los derechos humanos, si se debe hacer desde el propio Estado en solitario o bien, es recomendable contar con otras instituciones u organismos independientes como las Organizaciones No Gubernamentales (ONGs), incluyendo a las organizaciones privadas compuestas por voluntarios, los grupos comunitarios, las asociaciones profesionales comerciales, los sindicatos, las organizaciones académicas y científicas, etc. Estas entidades

pueden representar un papel esencial en la educación de los individuos para los derechos humanos y, por este motivo, el Estado tiene que estar obligado en un primer momento a proporcionar los recursos necesarios, tanto materiales como humanos en el sentido de proporcionar libertad de acción para el educador y libertad de elección para el educado, pues si consideramos los derechos fundamentales como necesidades básicas, casi instintivas, debemos pensar que los miembros de una sociedad elegirán siempre aquello que les proporcione la dignidad que les permite llamarse "seres humanos".

El sociólogo GEORGE HERBERT MEAD, de la escuela de Chicago, destacaba en sus trabajos[16] la influencia de la mente, el yo y la sociedad en las acciones e interacciones humanas. Este enfoque, conocido posteriormente como "interaccionismo simbólico", refleja la naturaleza activa y social de cada individuo en el grupo. La importancia del individuo como elemento "decisor" consciente, en relación con la materia de derechos humanos, nos acerca a la idea de que no son las instituciones políticas las que van a jugar un papel juegan un papel protagonista en la materialización de los derechos humanos, sino que lo son los propios individuos. La experiencia nos ha ido demostrando cómo allí donde existe una conciencia social de los derechos humanos, éstos se han respetado de forma generalizada, incluso sin la necesidad de una Constitución en el sentido más estricto. Sin embargo, esto no implica que en la práctica no se requieran normas y mecanismos que garanticen que ese respeto se mantenga, y es para este segundo momento cuando el Estado protector habría de manifestarse de nuevo, pero para limitar la inicial libertad de acción concedida. Podemos hablar de "validez de la norma" aún no existiendo para ella una previsión coactiva escrita y predefinida que obligue a que se cumpla lo estipulado en ellas, pero lo que es evidente es que para su eficacia práctica va a ser necesario el Estado. Eso sí, la educación y la acción social jugarán junto a él un importante papel para lograr tales objetivos.

[16] HERBERT MEAD, G. *La Génesis del Self y el control social*. Trabajo publicado por primera vez en *International Journal of ethics* (1925), e incluido después en *La filosofía del presente*, editado por "Clásicos del Pensamiento Social", CIS (2008). Se puede consultar, Ignacio Sánchez de la Yncera, en: http://dialnet.unirioja.es/servlet/fichero_articulo?codigo=758619&orden=81076

El papel de la educación en el desarrollo de las libertades es el de convertir meras declaraciones de intenciones en algo más, de forma que pasen de ser un ideal a un símbolo real respetado por un acuerdo común fijo en la conciencia social de los hombres. El esfuerzo individual para dirigir los actos propios, respetando o no las libertades de los demás, será siempre menor si el individuo está educado para ello, y entiende sus consecuencias, por este motivo es fundamental que las sociedades democráticas tengan un ideario configurado con valores jurídicos, políticos y éticos que orientados al disfrute efectivo de sus derechos y libertades, al disfrute en general de su existencia como sociedad, y así debe ser transmitido entre sus miembros.

Qué duda cabe pues que es necesario un sistema educativo abierto, internacionalizado, que sepa mostrar al individuo que además de ser ciudadano, es persona, que por ese motivo le asisten una serie de derechos, y que éstos no podrán ser ejercidos si no es en igual respeto a aquellos que junto a él conforman la sociedad en que vive.

Entonces las preguntas son las siguientes: ¿cómo podemos dar sentido a esa afirmación? ¿qué necesitamos para educar en derechos humanos? La respuesta es una, es necesario usar correctamente la información.

Hoy estamos en la "Sociedad de la Información", las comunicaciones han sufrido un desarrollo tan rápido que en muchos casos ni siquiera nuestra conciencia es capaz de asumirlo, pero lo cierto es que nuestras necesidades exigen nuevas formas de satisfacción y, es imprescindible tener datos para ello. Sólo manteniéndose informado el individuo tendrá la capacidad real de poder exigir sus propias garantías. En esta labor de información y conciencia, configurada como el último elemento de consolidación de un derecho fundamental en una sociedad, hay que considerar el papel de los centros escolares, pero en especial hay que destacar el que juegan las Organizaciones No Gubernamentales, respecto de la concienciación de los derechos. Realizan campañas de información para orientar no sólo a niños y jóvenes que se están formando como individuos, sino también para orientar a grupos de acción específica en la sociedad como jueces, los abogados, los

gobiernos, la policía, etc. También transmiten información relevante a Naciones Unidas, dando a conocer casos concretos de violaciones de los derechos humanos, participando en la creación de las Declaraciones de Derechos, en la creación, mejora y perfeccionamiento de las leyes, influyendo en las acciones de las instituciones políticas, en definitiva, ejerciendo su influencia y una importante presión social en la opinión pública, de ahí su crecimiento en número y su desarrollo en la especial materia que defienden.

La relevancia de estos organismos cobra fuerza cuando además de informar, se preocupan por formar a la sociedad, por hacer que sea consciente de que, si su forma de vivir ha cambiado y tiene nuevas necesidades de protección para nuevas formas de peligro, éstas existen y su "Estado protector" tiene la obligación de regularlas para que cada individuo pueda desarrollar su libertad de forma autónoma en la nueva "sociedad" en que vive. El ejemplo es hoy una realidad, las Nuevas Tecnologías implican ventajas para el desarrollo de la Humanidad, pero también suponen inconvenientes cuando coartan las libertades individuales con ataques de tan distinto signo que ciertamente no se alcanzan a ver hasta que el daño está hecho. La libertad física que se defendía por los revolucionarios franceses ha derivado hoy en lo que se podría llamar la "libertad virtual", que requiere ser respetada en la misma proporción que antes exigía la libertad física. Sobre esto se hablará más adelante, pero sirva como base para entender la aparición de ONGs[17] integradas en el avance tecnológico y preocupadas por lo que ocurre en este mundo paralelo y cuyos efectos pueden ser también devastadores para la dignidad del ser humano. Esta labor de las ONGs en el

[17] Así lo hacía por ejemplo la pionera Comisión de Libertades e Informática en España, organización no gubernamental, preocupada por la protección del individuo en la sociedad de las nuevas formas de peligro a que se enfrenta su libertad, y entre cuyos objetivos se encontraban: promover las medidas necesarias para dar a conocer toda violación, infracción, limitación o menoscabo del derecho a la protección de los datos personales y/o de las libertades individuales derivadas de un mal uso de la informática. Promover la asistencia y defensa a las víctimas de las infracciones o limitaciones en sus derechos y/o de las libertades individuales derivadas de un mal uso de la informática, con los medios de que pueda disponer. Promover el estudio y divulgación de dicho derecho y libertades, mediante la celebración de convenciones, jornadas, cursos, etc. y la publicación de libros, manuales o artículos sobre los mismos. En concreto, el artículo 5.5 de los Estatutos de la Comisión de Libertades e Informática, de 25 de noviembre de 2003, dispone: "Promover, ante los distintos órganos de representación social, instituciones, administraciones públicas y entidades privadas, la adopción o impulso de medidas de tipo legislativo, judicial, administrativas, sociales y cuantas actuaciones sean necesarias para la defensa, divulgación y fomento del derecho a la protección de los datos personales y/o de las libertades individuales derivadas de la práctica torticera o viciada del uso de la informática así como el restablecimiento de los derechos violados, el resarcimiento a los perjudicados por dichas acciones y la persecución y castigo de los responsables de tales violaciones o infracciones".

impulso, la educación y la consolidación en la conciencia de los individuos de sus derechos fundamentales con una referencia a la consideración que de estas organizaciones se tiene en las Naciones UNIDAS: "Las ONG son participantes de primerísima importancia en la defensa de los derechos humanos: representan y protegen a las víctimas, ofrecen servicios de expertos, reúnen y difunden información y alientan la educación sobre los derechos humanos. Entre las más activas ONG dedicadas a los derechos humanos se cuentan, en la actualidad, los grupos de mujeres. Estos desempeñan una función esencial en el adelanto y habilitación de la mujer, al concienciar sobre cuestiones de interés para la mujer y educar a las mujeres sobre sus derechos humanos. Muchas otras ONG trabajan de manera indirecta en defensa de los derechos humanos. Aunque se concentran principalmente en otras cuestiones, han incorporado a sus actividades los derechos humanos y ayudan al fomento de éstos mediante, entre otras cosas, la asistencia jurídica a grupos vulnerables"[18].

3.- Límites.

Se ha mostrado una definición "dualista"[19] de los derechos fundamentales que puede estar referida a cualquier momento histórico, y responder coherentemente a las cuestiones que pueda plantear su ejercicio efectivo, con valores y normas.

Se ha planteado también que, para entender consolidado un derecho fundamental, deben concurrir una serie de circunstancias concretas que lo hagan realizable, en el sentido de garantizar la satisfacción de las necesidades del individuo en cada momento social o histórico.

---

[18] Documentos de información de las Naciones Unidas. *Los Derechos Humanos hoy día: Una Prioridad de las Naciones Unidas. Los derechos humanos en acción.* Disponible en: http://www.un.org/spanish/hr/HRToday/action.htm [2005, 22 de abril].

[19] "Concepción dualista": nivel filosófico (valores al servicio de la persona humana) y nivel jurídico (inserción de los valores en normas jurídicas). PECES–BARBA, G. *Derechos Fundamentales*. Ed. Latina Universitaria. Madrid, 1980. pp. 24 y ss.

Ahora conviene analizar el alcance y límites de esas circunstancias, para su ejercicio efectivo, ya que no siempre supuso un mismo esfuerzo adaptar el contenido esencial de los derechos a la sociedad vigente en cada momento. Es una tarea que exige articular los derechos para la convivencia y el "orden público", y en ese objetivo la Constitución establece el contenido esencial de cada uno de los derechos fundamentales, establece los principios para su desarrollo legislativo (leyes que marcan los límites de su acción frente a terceros)[20] y, ordena los poderes del Estado como garantes de su ejercicio. Y, todo ello, bajo el control jurisprudencial de su constitucionalidad.

El ejercicio de los derechos y libertades ha de tener unos máximos y unos mínimos que hagan posible articular todas sus piezas, asumiendo (usando términos económicos) el menor coste de oportunidad en la materialización de sus beneficios. Un sistema constitucional coordinado y coherente no puede renunciar a la protección de un bien jurídico fundamental, inherente a la dignidad de la persona, sin existir de por medio un interés legítimo superior y una proporcionalidad que lo establezca como necesario[21]. En este sentido, las normas (delimitan) y una estructura política estable (garantía), deben definir el escenario adecuado de realización de los derechos fundamentales, pudiendo ser incorporados a la realidad, siempre bajo el control del Tribunal Constitucional.

Los derechos fundamentales son al fin y al cabo "exigencias de poder social, cuya toma de conciencia en cada momento histórico logra que los individuos y grupos sociales, manifiesten los valores fundamentales. Esto supone la pretensión de garantizarlos, ya sea por la vía institucional, o a través de medios extraordinarios"[22].

---

[20] STC 5/1981 (F.Jº. 7º) los derechos "tienen límites necesarios que derivan de su propia naturaleza, con independencia de los que se producen por su articulación con otros derechos o de los que, respetando siempre su contenido esencial, puede establecer el legislador".

[21] STC 292/2000 (F.Jº. 11º). "Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero, F.Jº. 6º; 18/1999, de 22 de febrero, F.Jº. 2º)".

[22] Definición extraída del Curso de Derechos Humanos publicado por el Instituto de Estudios Políticos para América Latina y África. Disponible en: http://www.iepala.es/curso_ddhh/ddhh33.htm [27 de abril de 2005].

Aunque los primeros textos[23] que reconocieron los derechos humanos se inspiraban en una tradición iusnaturalista de derechos absolutos e ilimitados, la doctrina pronto adoptó el concepto de "libertas" del Derecho romano, por el que la libertad sin límites implica una privación injusta de libertad para todos los demás[24]. Así lo explican FERNÁNDEZ-GALIANO y DE CASTRO CID[25], al señalar que "de una parte, la fundamentación iusnaturalista que inspiró aquellos primeros textos – fundamentación que, en alto grado, era tributaria del concepto racionalista del Derecho natural y singularmente del pensamiento de Locke- abonaba la tesis de que cualquier restricción de los derechos humanos resultaba ser "contra natura"; de otro lado aquel fue el momento en que la Historia empezó a cerrar el periodo de los poderes absolutos, se iniciaban los regímenes constitucionales, se abría el horizonte de la libertad y, una vez más, se hizo presente el "fervor del neófito" para enaltecer hasta la sublimidad unos derechos recién adquiridos".

La Declaración de los Derechos del Hombre y del Ciudadano del 26 de Agosto de 1789[26], explicaba claramente cuál es la razón de reconocer límites a los derechos fundamentales, y traduce "el límite de su naturaleza" como elemento configurador de cada derecho:

> Artículo 4º - "La libertad consiste en poder hacer todo aquello que no perjudique a los demás. Así pues, el ejercicio de los derechos naturales de cada hombre no tiene otra limitación que aquella que garantice el ejercicio de iguales derechos al resto de los miembros de la sociedad. Sólo la ley puede establecer estas limitaciones"[27].

---

[23] Declaración de derechos del buen pueblo de Virginia de 1776: S.1. "Que todos los hombres son, por naturaleza, igualmente libres e independientes, y tienen ciertos derechos inherentes, de los cuales, cuando entran en un estado de sociedad, no pueden ser privados ni despojados por ningún tipo de contrato entre estados; por ejemplo, el goce de la vida y de la libertad, junto a los medios de adquirir y poseer propiedades, y la búsqueda y obtención de la felicidad y la seguridad". Disponible en: http://www.icitizenforum.com/virginia-declaration-rights

[24] IGLESIAS-REDONDO, J. "En torno a la *libertas*". *Estudios en homenaje al profesor Juan Iglesias.* UCM. T. III. Madrid, 1988. pp. 1444 y 1446.

[25] FERNÁNDEZ-GALIANO, A. y DE CASTRO CID, B. Lecciones de Teoría del Derecho y Derecho Natural. Ed. Universitas. Madrid, 1993. p. 429.

[26] Declaración de los Derechos del Hombre y del Ciudadano de 1789. Disponible en: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/espagnol/es_ddhc.pdf

[27] Téngase en cuenta para la lectura de posteriores capítulos cómo se establece la "libertad" como el fundamento de cualquier sistema organizado de convivencia o sociedad, al que sólo la ley puede establecer limitaciones como su garantía que es.

Hoy se considera una evidencia que para garantizar el ejercicio de los derechos, es necesario limitarlos, en cuanto que sus titulares viven en sociedad y deben adaptarse a la convivencia pacífica y ordenada del Estado.

El "pactum libertatis" de LOCKE, o el "Contrato social" de ROUSSEAU, es el pacto que va a determinar la organización de la sociedad desde ella misma, y que lo va a materializar en el Estado y en las Constituciones. Las constituciones democráticas están basadas en el principio de que la soberanía reside exclusivamente en el pueblo, en el hecho de que la autonomía de la sociedad civil, y sus libertades, es lo que hay que salvaguardar y, para lograrlo, el consenso es el requisito principal pues sólo así puede darse el desarrollo efectivo de los derechos humanos. En este sentido el artículo 16 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789:

> Artículo 16º - "La sociedad en donde no estén garantizados los derechos ni esté establecida la separación de los poderes, carece de Constitución*".*

Es decir, el efectivo ejercicio de los derechos humanos requiere de una estructura adecuada que pueda sostener la articulación de los deberes y derechos de los ciudadanos.

Por tanto, la Constitución como instrumento responsable de ordenar la convivencia de los individuos, establecerá las bases que permitan limitar el ejercicio de los derechos fundamentales, ya sea en la definición de su contenido, ya sea en la previsión de los principios que deberán guiar su desarrollo legislativo, o el control judicial de su ejercicio. Además, organizará la actuación de los poderes públicos, del Estado como garante o protector del orden instaurado.

La jurisprudencia constitucional de los países occidentales coincide en afirmar que los derechos humanos son limitados.

Nuestro Tribunal Constitucional se manifiesta en este sentido diciendo que "como ya ha reiterado en diversas ocasiones este Tribunal, conviene tener presente, de una parte, que solo ante los límites que la propia Constitución expresamente imponga al definir cada derecho o ante los que de manera mediata o indirecta de la misma se infieran al resultar justificados por la necesidad de preservar otros derechos constitucionalmente protegidos, pueden ceder los derechos fundamentales (SSTC 11/1981, F.Jº. 7.º; 2/1982, F.Jº. 5.º; 110/1984, F.Jº. 5.º); y de otra que, en todo caso, las limitaciones que se establezcan no pueden obstruir el derecho "más allá de lo razonable" (STC 53/1986, F.Jº. 3.º), de modo que todo acto o resolución que limite derechos fundamentales ha de estar normativamente fundado y suficientemente motivado, ha de asegurar que las medidas limitadoras sean "necesarias para conseguir el fin perseguido" (SSTC 62/1982, F.Jº. 5.º; 13/1985, F.Jº. 2.º) y ha de atender a la "proporcionalidad entre el sacrificio del derecho y la situación en que se halla aquél a quien se le impone" (STC 37/1989, F.Jº. 7.º) y, en todo caso respetar su contenido esencial (SSTC 11/1981, F.Jº. 10; 196/1987, fundamentos jurídicos 4.º, 5.º, 6º; 197/1987, F.Jº. 11)"[28].

A nivel europeo, el TJCE confirma esta teoría respecto del derecho comunitario, entendiendo que los derechos fundamentales deben ser valorados en relación con su función social, y sobre ello, establecer límites de forma ponderada, pues "lejos de aparecer como prerrogativas absolutas, deben considerarse a la vista de la función social y de los bienes y actividades protegidos", de tal forma que, "los derechos de este tipo no se garantizan normalmente más que a reserva de las limitaciones previstas en aras del interés público"[29].

[28] STC 137/1990, de 19 julio de 1990 (F.Jº. 6º).

[29] "Considerando que, si bien es cierto que el régimen constitucional de todos los Estados miembros asegura la protección del derecho de propiedad y existen garantías similares del libre ejercicio del comercio, del trabajo y de otras actividades profesionales, la protección de tales derechos, lejos de convertirlos en prerrogativas absolutas, significa que hay que considerarlos a la luz de la función social de los bienes y actividades protegidos; que, por tal razón, esta categoría de derechos sólo se garantiza por regla general a reserva de las limitaciones establecidas en aras del interés público; que, en el ordenamiento jurídico comunitario, también parece legítimo mantener, respecto a tales derechos, determinados límites justificados por los objetivos de interés general perseguidos por la Comunidad, siempre y cuando no se atente contra la esencia de dichos derechos". STJCE de 14 de Mayo de 1974 . Asunto 4/73, Nold Kohlen- und Baustoffgrosshandlung. Rec. 1974. Apdo. 14. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61973CJ0004:ES:PDF

El Convenio para la Protección de los Derechos Humanos y, de las libertades Fundamentales (CEDH), señala en los párrafos 56 y 57 de su Memoria explicativa que es necesario establecer los límites, orientados a proteger los valores fundamentales de una sociedad democrática. Señala además que estos límites están sujetos al cumplimiento de una serie de circunstancias imprescindibles:

1. que la limitación sea impuesta por una norma legal,
2. que sea interpretada restrictivamente,
3. que lo sea con un fin legítimo, también previsto por una norma legal,
4. que sea una medida necesaria para la sociedad concreta de cada momento y lugar[30].

Se reconoce que los límites al ejercicio de los derechos fundamentales deben imponerse en favor del interés público y, por la necesidad de proteger otros bienes igualmente reconocidos constitucionalmente, lo que en un Estado de Derecho, no puede sino venir de la mano del legislador[31] y ser controlado, por el Tribunal Constitucional. Se acepta pues que la Ley sea quien desarrolle las condiciones ideales de su vigencia, en función de su contenido esencial o su propia naturaleza, sí como los límites a su ejercicio frente a terceros. También se acepta que, en función de esto, el Estado sea quien proporcione el espacio de "orden público"[32] más adecuado para su ejercicio.

Los límites a las posibilidades de ejercicio de un derecho van a venir en principio marcados por su propia naturaleza, según las particularidades que le prevea la norma para definir su contenido esencial. Por ejemplo, el derecho de asociación, requiere del consenso de dos personas o más, lo que

[30] MARTÍNEZ MARTÍNEZ, R. *Tecnologías de la Información, Policía y Constitución*. Ed. Tirant lo Blanch. Valencia, 2001. pp. 153 – 155.
[31] HÄBERLE, P. *La garantía del contenido esencial de los derechos fundamentales.* Traducción de Brage Camazano, J. Ed. Dykinson. Madrid, 2003. pp. 169 y ss.
[32] (...) "no todos los derechos deben de tener restricciones, sólo aquellos que entran en conflicto con otros derechos o implican una materialización de los actos de los hombre. Por ejemplo tenemos la libertad de conciencia, la cual sólo al incidir en el aspecto interno del hombre, no tiene razón de ser el establecer alguna limitación". VIDAL GÓMEZ ALCALÁ, R. *La Ley como límite de los derechos fundamentales.* Ed. Porrúa. México, 1997. p. 91.

significa que cada una de ellas va a ser titular del derecho en sí, pero no va a poder ejercitarlo efectivamente si no se da la condición de consenso entre ellas. Y en este sentido, la "ejecución legislativa", contribuirá a dotarlos de contenido y garantías frente a terceros, siempre vinculada a la Constitución y bajo el control del Tribunal Constitucional[33].

El Estado está sometido al imperio de la ley; el "Estado de Derecho" proporciona la fórmula más adecuada para el ejercicio de los derechos fundamentales y de sus límites, y ello es así, tanto desde un punto de vista liberal como social: "El Estado liberal de Derecho pretende garantizar la libertad, la propiedad, la igualdad, la seguridad jurídica y los derechos de participación política. En cambio, el Estado Social, además de mantenerlos y de preocuparse por su efectividad material, se responsabiliza de que se entiendan a la generalidad de los individuos"[34]. Pero no podemos olvidar que no podrá ser efectivo, si no se mantiene en perfecto equilibrio el juego de la separación de poderes de MONTESQUIEU, diseñado para favorecer la dignidad y la libertad de los ciudadanos por la vía de la limitación del poder.

Para CARL SCHMITT[35], y siguiendo la idea de que el Estado de Derecho se basa precisamente en el imperio de la ley, el "Estado legalitario" ha de reposar sobre dos principios elementales: los derechos fundamentales como presupuestos a la autoridad del Estado y la división de poderes. El primero, postula la libertad del individuo como algo anterior al Estado, y el segundo, determina que el poder del Estado se divide en un sistema de competencias limitadas. Y en este contexto, el imperio de la ley no se postula sólo para garantizar una protección efectiva frente a los abusos que el Poder haga de sus atribuciones, sino que también se establece para marcar sus pautas de actuación, ("el buen gobierno") en su objetivo de garantizar, para los miembros de la sociedad, las condiciones de vida apropiadas.

---

[33] HÄBERLE, P. *La garantía del contenido…* Op. Cit. pp. 172, 186 y 187.

[34] DE ASÍS ROIG, R. *Valores, derechos y Estado a finales del S.XIX*. Edición y Prólogo de Eusebio Fernández García. Universidad Carlos III de Madrid. Ed. Dykinson. Madrid, 1996. p. 93.

[35] (...) "derechos fundamentales y división de poderes designan pues el contenido esencial del elemento típico del estado de derecho, presente en la Constitución". SCHMITT, C. *Teoría de la Constitución*. Alianza Editorial. Madrid, 2001. p. 139. Cfr. Editorial "Revista de Derecho Privado", 1934.

En resumen, la Constitución recoge límites a los derechos fundamentales, con la mera definición de su contenido esencial, pero también, al prever los principios que deben regir el desarrollo legislativo (y el control judicial) de su ejercicio frente a terceros. Asimismo, es el pacto que determina la organización política que debe garantizar el sistema constitucionalmente establecido para la protección y garantía de esos derechos, en aras de la consecución del "orden público".

3.1.- La Ley.

Una vez sentado que los derechos y libertades no son absolutos o ilimitados y, considerada la Ley como instrumento esencial del desarrollo de su contenido esencial, hay que analizar el papel que desempeña en la determinación de las circunstancias que deben darse para justificar la limitación de un derecho fundamental, ya que "la motivación próxima que impulsa a la sociedad a la creación de normas jurídicas radica en la necesidad de garantizar a toda costa la seguridad jurídica del individuo"[36].

BOBBIO, en su tesis del reconocimiento de las "garantías" frente a límites injustos, como elemento esencial de la existencia de un derecho, destacaba la necesidad de su positivación, porque la convivencia humana supone, o así debe ser, la aceptación de una serie de usos y pautas por las que se gobierna la comunidad, y se impone por tanto la evidencia de que un determinado orden debe regir la conducta social del individuo.

El reconocimiento constitucional de los derechos fundamentales, de su contenido esencial, responde a criterios históricos y a determinados principios organizativos y políticos, porque debe responder a las necesidades de sus destinatarios en el momento concreto en que vayan a ser ejercidos.

[36] ALBÁCAR LÓPEZ, J. L. *Protección de los derechos fundamentales en la nueva Constitución Española*. Texto de la ponencia española en la IV conferencia de Tribunales Constitucionales. Serie Discursos (Octubre). Ed. Panorama. Viena, 1978. p. 13.

Su papel es coordinar el reconocimiento normativo de su contenido esencial, y el ejercicio de los derechos, considerando los límites que mediatizarán su efectividad frente a terceros[37].

En cuanto a los límites que vienen dados por su definición, por su contenido, o por su propia naturaleza, IGNACIO DE OTTO señala que la mayoría de las cuestiones sometidas al TC en materia de límites a los derechos fundamentales, son en realidad un problema de configuración del contenido, "de delimitación conceptual del contenido mismo del derecho, de forma que lo que se llama protección de otro bien constitucional no exige en realidad una limitación externa de los derechos y libertades, porque las conductas de las que deriva la eventual amenaza del bien y de cuya protección se trata sencillamente no pertenecen al ámbito del derecho fundamental y, en consecuencia, no se requiere ninguna limitación de éste para excluirlas"[38]. Este autor, considera que el contenido de un derecho fundamental, no es sólo el que muestra su propia definición legal, sino que lo es aquel que deriva de una interpretación unitaria y sistemática de todas las normas de la Constitución. Así, considerando la rigidez propia de un texto normativo, la labor del legislador constitucional debería verse como una tarea "de razón", de análisis y comprensión del grupo en cada momento, que le permita formular sus derechos de forma sencilla, clara y precisa, pero también coherentes con el resto.

En opinión de JIMÉNEZ CAMPO, es preciso incluso evitar "el aparente absurdo de admitir que el legislador pueda limitar un derecho creado por la Constitución y percibir con mayor claridad la contribución del legislador a la definición de los derechos[39]". Sin embargo, BRAGE CAMAZANO, considera que "no es ningún absurdo, ni real ni puramente aparente, que el legislador limite los derechos fundamentales "creados" por la Constitución, pues es también ésta la que autoriza la esa limitación, aunque sólo bajo unas

[37] La buena fe como límite de los derechos fundamentales, en una Constitución que descansa sobre el principio de la libertad personal como una libertad de la autonomía de la voluntad. OTTO Y PARDO de. I. *La regulación del ejercicio de los derechos y libertades. La garantía de su contenido esencial en el artículo 53.1 de la Constitución. Derechos fundamentales y Constitución*. Ed. Civitas. Madrid, 1988. pp. 103 – 106.
[38] Ibídem. p. 137.
[39] JÍMENEZ CAMPO, J. *Derechos fundamentales, concepto y garantías.* Ed. Trota. Madrid, 1999. p.39.

condiciones estrictas y entre ellas, la sólo aparentemente paradójica vinculación al contenido constitucional de tales derechos del legislador, lo que no supone ignorar en modo alguno, por cierto la contribución del legislador a la "definición" de los derechos fundamentales, porque cuando el legislador limita un derecho, también está contribuyendo a definirlo y está introduciendo en la vida social sus propias concepciones políticas, por más que éstas tengan, por la propia naturaleza y fuerza de los derechos fundamentales, un campo de juego más estrecho que en otros campos"[40].

En cuanto a los límites que implican los principios constitucionales que guían el desarrollo legislativo de los derechos fundamentales, hay que entenderlo como una "intervención" del derecho, en el sentido de restricciones a su ejecución.

Según BRAGE CAMAZANO, esta restricción es una técnica propia del Estado de Derecho para diferenciar entre las actuaciones de los poderes públicos para "intervenir" y restringir las posibilidades de su ejercicio, y las actuaciones dirigidas simplemente a desarrollar el derecho, a precisar su contenido o, a articular su defensa a través de los cauces procesales oportunos. Por eso, cuando se señala la Constitución como el instrumento adecuado para fijar las circunstancias de su ejercicio (límites), así como los mecanismos, normas y/o garantías necesarios para ello, es porque fija los dictados básicos de la convivencia social[41].

Según GARCÍA DE ENTERRÍA, la Constitución "no es sólo el emblema de la Comunidad, es también, y de manera especialmente intensa o "más fuerte", la norma superior de garantía, eficaz en todas las relaciones jurídicas imaginables"[42], materializa las circunstancias del orden social que gobierna. No es un mero programa difuso o abstracto de objetivos para la comunidad, sino una guía de aplicación directa sobre los individuos que deciden dotarse

[40] BRAGE CAMAZO, J. *Los límites a los derechos fundamentales*. Ed. Dykinson. Madrid, 2004. p. 276.
[41] Sobre instrumentos legales, o procesal-judiciales, y sobre su fuerza ejecutiva en la protección de los derechos, véase BLANC ALTEMIR, A. *La protección internacional de los derechos humanos a los cincuenta años de la Declaración Universal*. Ed. Tecnos. Madrid, 2001. Y, CARRILLO SALCEDO, J. A. *Soberanía de los Estados y derechos humanos en Derecho Internacional*. Ed. Tecnos. Madrid, 2001.
[42] GARCÍA DE ENTERRÍA, E. "La Constitución juzgada por los juristas". *Estudios sobre la Constitución Española*. Monografías, nº 7. Instituto de Derechos Humanos Bartolomé de las Casas. Universidad Carlos III. Madrid, 1994. p. 119.

de ella y aceptar lo que se estipula en sus preceptos. Y habrá "Norma Fundamental", si existe el compromiso de la Sociedad (se da por celebrado de manera eficaz el contrato social), sea o no por escrito, y sea con el reconocimiento expreso del derecho fundamental, o con el reconocimiento del sistema protector, en igual o diferente precepto normativo. Determinados regímenes normativos, como lo es el vigente en países anglosajones, carecen de Constitución como norma escrita, pero no por ello puede decirse que no reconozcan los derechos fundamentales del hombre, sino que más bien, delimitan y concretan su alcance en normas de diferente rango al que se considera para las Cartas Magnas. En todo caso, el objetivo y el resultado son similares: reconocer y respetar los derechos humanos.

En general, serán las normas elaboradas por el poder legislativo las encargadas de establecer en qué sentido se debe entender su núcleo esencial y las garantías de su ejercicio, pero será la justicia constitucional quien controle que efectivamente sea así.

Y es que el desarrollo legislativo de la Constitución obedece a la necesidad de un sistema flexible y progresivo que conozca bien la realidad social que se quiere regular. Ella misma prevé ese desarrollo[43] dentro del respeto al contenido esencial del derecho fundamental, así como el carácter o rango de la norma que asuma esta función, exigiendo que sea de un nivel superior entre las demás. Es tarea propia de la Ley que los cambios queden positivados en las normas, ya que la naturaleza de un derecho fundamental se corresponde con el valor moral y social que quiere preservar en el momento histórico concreto; pero también es su tarea el conciliar sus límites y las soluciones ante un conflicto en su realización, respecto de otros derechos de igual categoría (por actuaciones del propio individuo que protegen, de otros individuos en similar situación, o por actuaciones del propio Estado).

[43] Artículo 53.1 CE: "Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos".

VIDAL GÓMEZ ALCALÁ[44] considera que, de entre los elementos delimitadores del ejercicio de los derechos, el ejemplo típico es la Ley, pero que "como límite a los Derechos Fundamentales, es en sí un límite impreciso, y es en realidad ocioso, y su inclusión, a nivel constitucional, hace peligrar el derecho fundamental al que se le impuso dicha limitación, así como a los restantes principios y valores reconocidos a nivel constitucional (...) que hace peligrar". También hay quien refuerza este argumento diciendo que la limitación de los derechos por la Ley desvirtúa la supremacía jurídica que deben tener[45].

Pero en todo caso, de lo que no hay duda, es de que la Ley[46], como instrumento de aplicación de la norma constitucional, puede limitar el ejercicio de los derechos fundamentales en defensa y protección de otros intereses de superior consideración y que, como reconoce el propio VIDAL GÓMEZ ALCALÁ, "la función de la norma, cuando limita externamente un derecho fundamental, es aplicar ese principio moral, si lo hace, tal límite estará justificado, si no lo hace así, no lo estará".

La tarea de delimitación y limitación del contenido esencial de un derecho fundamental, es descrita por el TC en su STC 140/1986 (F.Jº. 5º), al decir que "El desarrollo legislativo de un derecho proclamado en abstracto en la Constitución consiste, precisamente, en la determinación de su alcance y límites en relación con otros derechos y con su ejercicio por las demás personas, cuyo respeto, según el artículo10 CE es de los fundamentos del orden político y de la paz social. Pero acepta igualmente que no toda limitación es posible[47] como ya ha reiterado en diversas ocasiones este Tribunal, conviene tener presente, de una parte, que sólo ante los límites que

[44] VIDAL GÓMEZ ALCALÁ, R. *La Ley como límite...* Op. Cit. p. 199.
[45] Ibdem. p. 201. El autor RODOLFO VIDAL cita a K. LOEWENSTEIN, su obra *Teoría de la Constitución* (1983).
[46] STC 120/1990 (F.J. 8º) "conviene tener presente, de una parte, que sólo ante los límites que la propia Constitución expresamente imponga al definir cada derecho o ante los que de manera mediata o indirecta de la misma se infieran al resultar justificados por la necesidad de preservar otros derechos constitucionalmente protegidos, puedan ceder los derechos fundamentales (SSTC 11/1981, F.Jº. 7º; 2/1982, F.Jº. 5º, 110/1984, F.Jº. 5º), y de otra que, en todo caso, las limitaciones que se establezcan no pueden obstruir el derecho "más allá de lo razonable" (STC 53/1986, F.Jº. 3º), de modo que todo acto o resolución que limite derechos fundamentales ha de asegurar que las medidas limitadoras sean "necesarias para conseguir el fin perseguido" (SSTC 62/1982, F.Jº. 5º; 13/1985, F.Jº. 2º)y ha de atender a la "proporcionalidad entre el sacrificio del derecho y la situación en que se halla aquel a quien se le impone".
[47] STC 137/1990, F.J. 6º.

la propia Constitución expresamente imponga al definir cada derecho o ante los que de manera mediata o indirecta de la misma se infieran al resultar justificados por la necesidad de preservar otros derechos constitucionalmente protegidos, pueden ceder los derechos fundamentales (SSTC 11/1981, F.Jº. 7.º; 2/1982, F.Jº. 5.º; 110/1984, F.Jº. 5.º); y de otra que, en todo caso, las limitaciones que se establezcan no pueden obstruir el derecho "más allá de lo razonable" (STC 53/1986, F.Jº. 3.º), de modo que todo acto o resolución que limite derechos fundamentales ha de estar normativamente fundado y suficientemente motivado, ha de asegurar que las medidas limitadoras sean «necesarias para conseguir el fin perseguido» (SSTC 62/1982, F.Jº. 5.º; 13/1985, F.Jº. 2.º) y ha de atender a la «proporcionalidad entre el sacrificio del derecho y la situación en que se halla aquél a quien se le impone" (STC 37/1989, F.Jº. 7.º) y, en todo caso, respetar su contenido esencial (SSTC 11/1981, F.Jº. 10º; 196/1987, F.Jº. 4.º, 5.º, 6º; 197/1987, F.Jº. 11º)".

Hasta aquí se entiende que la Constitución recoge el contenido esencial de los derechos fundamentales y los principios básicos de su interpretación y desarrollo, como límites que debe respetar el poder legislativo, a la hora de desarrollar las circunstancias o condiciones de su ejercicio frente a terceros, sin realizar una clasificación de dichos límites.

En este sentido, por ejemplo, el profesor PECES-BARBA habla de la existencia de una serie de límites generales a los derechos fundamentales[48]:

1.- La moral básica (artículo 1.1 CE).

2.- Los bienes constitucionales (también en Leyes Orgánicas y principios de organización política).

3.- El límite del derecho ajeno.

4.- La buena fe y el abuso del derecho.

Pero BRAGE CAMAZANO, prefiere considerar una distinción entre límites explícitos y límites implícitos[49]. Así, distingue como límites explícitos

[48] PECES-BARBA, G. *Curso de derechos fundamentales*, BOE/Universidad Carlos III. Madrid, 1993. pp. 590 y ss. Al respecto, BRAGE CAMAZANO, J. en *Los límites…* Op.Cit. p. 297, no reconoce esta clasificación porque no es aplicable, de forma general, a todos los derechos ni a todos los casos. Para este autor, los límites son siempre particulares de cada derecho.

los criterios que determine de forma proporcionada el legislador para la restricción de derechos en aras de su protección, sin conculcar de forma injusta o estrictamente necesaria otros derechos de igual naturaleza. También, lo son aquellas restricciones conceptuales, es decir las palabras utilizadas para su definición (información "veraz", inviolabilidad de domicilio excepto "consentimiento del titular", reuniones "pacíficas y sin armas", etc.). O las restricciones que se establecen sobre el titular (ciudadanos, extranjeros, menores de edad, etc.).

Como límites implícitos, "aquellos que se derivan de la coexistencia de los derechos fundamentales entre sí o con otros bienes constitucionales y que no están previstos de manera expresa en el texto constitucional"[50], señala a modo de ejemplo, la moral respecto al derecho a un proceso público, o la protección a la juventud y la infancia como límites al derecho a la libertad de expresión. La Sentencia STC 62/1982 de 15 de Octubre, en relación con el primero, sostiene que los límites implícitos reconocidos por el Derecho Internacional se insertan en nuestra Constitución, marcándole límites como éste de la moral. Y ello porque, a través de un largo proceso evolutivo del Estado de Derecho en Europa, dónde el valor de la Declaración Universal de los Derechos Humanos es similar, para las Naciones Unidas, al de una Constitución en un Estado, existe un reconocimiento de los derechos humanos a nivel internacional, con sus límites y con sus condiciones de ejercicio efectivo en la comunidad. El preámbulo de esta declaración explica uno de sus principales objetivos: "reafirmar la fe en los derechos fundamentales del hombre" a través de un programa o listado, instrumentando el alcance de su ejercicio a través de una serie de pactos, que instauren y consoliden su respeto con validez general. Sin entrar a valorar el carácter vinculante de esta norma o de mera recomendación, basta su sólo reconocimiento como "compromiso" de la Comunidad Internacional, como un "Contrato Social" que compromete a quien lo ratifica y que establece pautas también de interpretación para el derecho interno de los Estados miembros.

---

[49] BRAGE CAMAZANO, J. en *Los límites…* Op.Cit. pp. 303 y ss.
[50] Ibídem. p. 308.

Pero, independientemente de la clasificación que quiera hacer de los límites, ya sea con alcance general o con alcance restrictivo, lo verdaderamente relevante va a ser la determinación de las condiciones que permitan llevar a cabo tales limitaciones.

Respecto de los límites propios de la naturaleza o contenido de un derecho fundamental, esa condición será básicamente el "orden público" que instaure la Constitución.

Respecto de los límites que quepa establecer para el ejercicio de los derechos frente a terceros, el Tribunal Constitucional los ha fijado de forma general en: la reserva de Ley, el principio de proporcionalidad y, el contenido esencial.

Según el "principio de reserva de Ley" del artículo 53 de la CE, el desarrollo legislativo marcará los límites de las posibilidades de ejercicio de los derechos fundamentales frente a otros derechos de igual calidad con los que pudieran encontrarse en conflicto[51], así como de la intervención de los poderes públicos en su contenido esencial. Y corresponderá al Tribunal Constitucional su control según lo dispuesto por el artículo 9.3 CE, que determina el principio de legalidad y de seguridad jurídica, frente a la actuación de los poderes públicos[52].

Así lo ha definido en numerosas ocasiones la jurisprudencia constitucional, por ejemplo, en materia de secreto de las comunicaciones y protección de datos, destaca por ejemplo la STC 49/1999, de 5 de abril, que señala en su F.Jº. 4º que "por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (artículo 81.1 CE), o limite o condicione su ejercicio (artículo 53.1 CE), precisa una habilitación legal". Pero no, de cualquier tipo, sino que, habrá de estar prevista la restricción, en una Ley de "singular precisión" (STC 49/1996, F.Jº. 3º). La STC 292/2000, de 30 de Noviembre, ha señalado en su F.Jº. 11º, que una

[51] STC 104/2000, de 13 de abril, (F.Jº. 8º).
[52] SSTC 11/1981, (F.Jº. 5º) y 196/1987, (F.Jº. 6º).

ley será contraria a un derecho fundamental "cuando se limite a apoderar a otro poder público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese poder público (…) esgrimiendo incluso intereses que no son protegidos con rango constitucional (…) De ser ese el caso, la Ley habrá vulnerado el derecho fundamental en cuestión, ya que no sólo habrá frustrado la función de garantía propia de toda reserva de ley relativa a derechos fundamentales al renunciar a fijar por si misma esos límites, dado que la reserva de ley impone al legislador, además de promulgar esa ley, regular efectivamente en ella la materia objeto de la reserva ; sino también al permitir que el derecho fundamental ceda ante intereses o bienes jurídicos de rango infraconstitucional en contra de lo dispuesto en la propia Constitución, que no lo prevé así".

El "principio de proporcionalidad", significa que la aplicación de límites a los derechos fundamentales, implica necesariamente una concordancia práctica o equilibrio con el resto del ordenamiento jurídico, a fin de no privar de significado a ningún otro derecho constitucional (entendiendo siempre la preeminencia de los derechos fundamentales). Este equilibrio debe tener en cuenta que las medidas que se adopten, bien para el ejercicio del derecho, bien para su restricción, han de ser estrictamente necesarias para el fin que se quiere conseguir, sin que quepa otra alternativa. En materia de protección de datos, la STC 171/1999, de 27 de septiembre de 1999, señala en su F.Jº. 10º: "que se tiene que tratar de un mecanismo de orden preventivo para la protección del derecho (SSTC 160/1991, F.Jº. 8º), de forma que lejos del automatismo formal en la concesión, la autorización debe expresar la ponderación de las circunstancias y los intereses, público y privado, en conflicto (SSTC 160/1991, F.Jº. 8º; 50/1995, F.Jº. 5º) "para decidir en definitiva si merece el sacrificio de éste, con la limitación consiguiente del derecho fundamental" (STC 50/1995, F.Jº. 5º). Y la STC 126/2000, de 16 de Mayo, señala en el F.Jº. 6º que, en el ámbito de las escuchas telefónicas, nuestra doctrina[53], mantienen que una medida

[53] SSTC 81/1998, de 2 de abril, F.Jº. 5º, 121/1998, de 15 de junio, F.Jº 5º, 151/1998, 49/1999, FF.JJº. 7º y 8º, 166/1999, F.Jº. 2º, 171/1999, F.Jº. 5º, 236/1999, de 20 de diciembre, F.Jº. 3º) y la del Tribunal Europeo de Derechos Humanos [casos Klass (Sentencia 6 de septiembre de 1978), Malone (Sentencia 2

restrictiva del derecho al secreto de las comunicaciones sólo puede entenderse constitucionalmente legítima, desde la perspectiva de este derecho fundamental, si se realiza con estricta observancia del principio de proporcionalidad (STC 49/1999, F.Jº. 7º); es decir, si la medida se autoriza por ser necesaria para alcanzar un fin constitucionalmente legítimo, como –entre otros–, para la defensa del orden y prevención de delitos calificables de infracciones punibles graves, y es idónea e imprescindible para la investigación de los mismos"[54]. Por tanto, debe hacerse un juicio de idoneidad, intervención mínima y ponderabilidad, entre el fin perseguido, las medidas adoptadas y los derechos fundamentales en juego.

En cuanto al respeto al "contenido esencial" del específico derecho a la protección de datos", la STC 290/2000, de 30 de noviembre de 2000, lo define en el F.Jº. 7º, remitiéndose al su F.Jº. 8º de la STC 11/1981, de 8 de Abril (como propone el Defensor del Pueblo en sus alegaciones), y habla de dos posibilidades complementarias para entender este concepto previsto por el artículo 53 de la CE. Una opción es considerar su naturaleza jurídica y establecer una relación entre las palabras literales utilizadas y las "ideas generalizadas y convicciones generalmente admitidas entre los juristas", teniendo en cuenta el momento histórico en que evalúe y, que muchas veces "el tipo abstracto del derecho preexiste conceptualmente al momento legislativo". Recuerda el Alto Tribunal que el contenido esencial de un derecho subjetivo son "aquellas facultades o posibilidades de actuación necesarias para que el derecho sea recognoscible como pertinente al tipo descrito y sin las cuales deja de pertenecer a ese tipo y tiene que pasar a quedar comprendido en otro desnaturalizándose, por decirlo así". Otra opción, complementaria de la anterior, para definir el contenido esencial, es buscar "los intereses jurídicamente protegidos como núcleo y médula de los derechos subjetivos". Es decir, buscar aquello que es imprescindible para dar vida al derecho, para hacer que los intereses que se quieren proteger, efectivamente queden garantizados, y ello porque "se rebasa o se desconoce

---

de agosto de 1984), Kuslin y Huvig (Sentencia 24 de abril de 1990), Haldford (Sentencia 25 de marzo de 1998), Klopp (Sentencia 25 de marzo de 1998) y Valenzuela (Sentencia 30 de julio de 1998).

[54] STC 344/1990, de 1 de octubre; SSTC 85/1994, de 14 de marzo, F.Jº. 3º; 181/1995, de 11 de diciembre, F.Jº. 5º; 49/1996, de 26 de marzo, F.Jº. 3º; 54/1996, de 26 de marzo, FF.JJº. 7º y 8º; 123/1997, de 1 de julio, F.Jº. 4º; 49/1999, F.Jº. 8º y 166/1999, F.Jº. 5º; SSTEDH casos Huvig y Kruslin, y Valenzuela.

el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección".

Por último, la STC 290/2000 advierte que el legislador deberá determinar cuándo concurre "ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, y además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias"[55]. Igualmente considera que el derecho a la protección de datos no es ilimitado, y aunque no sea la misma Constitución la que le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación, han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, y ello según el principio de unidad de la Constitución.

3.2.- El Estado.

Según lo expuesto hasta ahora, la Constitución marca límites de los derechos fundamentales en la definición de su contenido esencial, y con la previsión de principios informadores de su desarrollo legislativo para el ejercicio frente a terceros.

Y en este marco, se ha presentado al Estado de Derecho "como un modelo articulador de las exigencias, en principio antagónicas, que reflejan las ideas de libertad y de ley, en cuanto imperativo de la comunidad social. La superación de esa antinomia sólo podría llegar a partir de una síntesis entre ambas nociones, para ello era necesario concebir a la Ley, no como un producto de arbitrio, sino de una voluntad general encaminada directamente a garantizar los derechos fundamentales de los individuos. Hacia esa síntesis

[55] STC 290/2000, F.Jº. 16º.

se dirigió la idea guía del Estado de Derecho"[56] de tal forma que es el garante del "orden público", que va a permitir el efectivo ejercicio de los derechos fundamentales.

Como decía el artículo 16 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789, "donde no estén garantizados los derechos ni esté establecida la separación de los poderes" no hay Constitución. Esta es la encargada de instituir la organización de los poderes del Estado Democrático, de imponer la sumisión de éstos al derecho interno, y de guiarles en la consecución del necesario "orden público", para poder hablar de derechos fundamentales.

El papel del Estado puede analizarse desde dos puntos de vista: como agente activo, garante y protector de la comunidad y, como agente pasivo, obligado a no injerir en los derechos fundamentales y valores de aquella sociedad constitucionalmente establecida. "En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona está solamente sujeta a las limitaciones establecidas por la Ley con el único fin de asegurar el reconocimiento y respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general de una sociedad democrática"[57]. Se puede decir que el Estado es garantía de los derechos fundamentales, y está a la vez limitado por su contenido esencial.

Los textos constitucionales que surgen a partir de finales del siglo XVIII, durante el siglo XIX, y sobre todo, a partir de la segunda mitad del siglo XX, ya contienen Derechos Humanos, fruto de una conciencia social nacida de las revoluciones francesas, que exige sean cubiertas una serie de necesidades propias de "una vida digna" y, exigen que para ello se instaure

[56] PÉREZ LUÑO, A. *Derechos Humanos, Estado de Derecho...* Op. Cit. p. 212.

[57] Artículo 29.2. Declaración Universal de Derechos Humanos, aprobada por la Asamblea General de Naciones Unidas, en su Resolución 217 A (III), el 10 de diciembre de 1948 en París. Texto original: "Dans l'exercice des ses droits et dans la jouissance de ses libertés, chacun n'est soumis qu'aux limitations établies par la loi exclusivement en vue d'assurer la reconnaissance et le respect des droits et libertés d'autrui et afin de satisfaire aux justes exigences de la morale, de l'ordre public et du bien-etre général dans une société démocratique". Disponible en: http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/043/88/IMG/NR004388.pdf?OpenElement

el Estado, limitado en su actuación por la moral, el orden público, y el bienestar general de la sociedad.

THOMAS HOBBES y JOHN LOCKE afirmaban[58] que los Derechos Humanos parten de un contrato social celebrado entre individuos, con la finalidad de contrarrestar el poder de un Estado agresivo. Pero también es un contrato entre los miembros de la sociedad. Esta concepción se ha ido matizando hacia un "contrato de intercambio", que consiste en que las partes ceden parcelas de sus derechos a cambio de obtener la protección del Estado en otros ámbitos que consideran prioritarios. Se trata de renunciar a una serie de garantías para poder ejercitar aquello que se considera indispensable para la vida en libertad, y que suelen variar al mismo ritmo que los cambios sociales. Así, desde la Declaración francesa de Derechos del Hombre y del Ciudadano de 1789, hasta la llamada "Constitución Europea"[59], muchas han sido las declaraciones de derechos que se han dictado tratando de conciliar los intereses en juego. Se han ido adoptando en los diferentes Estados[60] reconociendo tanto la necesidad de un Estado protector, como la necesidad de imponer límites a su capacidad de actuación, para lograr el objetivo del "orden público".

El Estado de Derecho implica un sistema de garantías sólido, pues son elegidas por el pueblo, y gestionadas para éste, para su interés general. Por este motivo, debe ofrecer una estructura institucional dotada de un sistema de justicia e información que aporte de forma dinámica las condiciones más adecuadas a cada momento, para la articulación tanto de los derechos y libertades consagrados, como de sus límites, ya que "las libertades nunca son definitivamente adquiridas y su defensa necesita de un

---

[58] POLIN R. *Politica y filosofía en Thomas Hobbes*. Prensas Universitarias de Francia. Paris, 1953 y 1999; y, LASSALLE, J.M. *Locke, liberalismo y propiedad*. Servicio de Estudios del Colegio de Registradores. Madrid, 2003.

[59] El proyecto de Tratado Constitucional de la UE fue abandonado después de que franceses y holandeses rechazaran en referéndum su aprobación en el año 2005.
Texto íntegro del "Tratado por el que se establece una Constitución para Europa" [DOUE 16 de Diciembre de 2004 (C310)] Disponible en:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:310:0001:0002:ES:PDF

[60] Son ejemplos destacados: la Declaración de Derechos del Hombre y del Ciudadano, Francia 1789; la Declaración Universal de Derechos Humanos, de la ONU 1948; la Declaración de los Derechos del Niño, de la ONU 1959; el Pacto Internacional de Derechos Civiles y Políticos, de la ONU 1966; la Convención Americana de Derechos Humanos,1969; la Convención Europea de Derechos Humanos, Roma 1950 o el Proyecto para una Constitución Europea. Roma, 2003.

esfuerzo permanente para evitar ese contraste entre lo que Bobbio llama las solemnes declaraciones y su realización, entre la grandiosidad de las propuestas y la miseria de los cumplimientos"[61].

LÓPEZ PINA considera "que si cobramos conciencia de que el Estado es el garante y simultáneamente la amenaza de la libertad individual, tenemos ante nosotros el auténtico dilema sobre el que debe definirse la interpretación constitucional. En principio el Estado es el garante de la libertad, ha creado y ejecuta la Constitución, a fin de hacerla realidad. O lo que es lo mismo: la libertad como derecho únicamente existe a través del Estado. Dependemos del Estado, que establece derechos fundamentales, los garantiza y los desarrolla en la realidad de cada momento. A la vez sin embargo, el Estado es en la comunidad el máximo poder; sólo él dispone de facultades soberanas. El Estado es superior al ciudadano y potencialmente siempre está en situación de amenazar la libertad individual. De ahí que debamos moderar las expectativas de que a fin de garantizar mayor libertad, ejerza aún más moderación, de que tal señorío puede también constituir un riesgo para la libertad"[62].

El significado de "Estado" debe entenderse además como una forma de organización política y vida ordenada, en el contexto del artículo 10 de la Constitución, cuando dice que "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 son fundamento del orden político y de la paz social". Y es que sólo existirá "orden público" constitucionalmente legitimado si se respeta la dignidad de los individuos, y el papel del Estado en la consecución de este orden y garantizar su permanencia estable. El "orden público" es tanto en un objetivo como un límite a la actuación del Estado. Es un elemento de garantía abstracta y formal del desarrollo integral del ser humano[63], con la misión de hacer respetar los derechos fundamentales.

---

[61] SÁNCHEZ FERRIZ, R.: "Algunas reflexiones sobre la efectividad de los derechos", *Revista de Derecho Político*, Nº 36. Ed. UNED, 1992. p. 238.

[62] LÓPEZ PINA, A. *La garantía constitucional de los derechos fundamentale*s. *Alemania, España, Francia e Italia.* Ed. Cívitas. Madrid, 1991. p. 248.

[63] DE BARTOLOMÉ CENZCANO, J. C. *El orden público como límite al ejercicio de los derechos y libertades*. Centro de Estudios Políticos y Constitucionales. Madrid, 2002. p. 99.

Siguiendo esta línea de pensamiento, HOBBES citaba al Estado en su "Leviatán" como "un monstruo necesario"; partiendo de la mitología hebrea, y dice que[64]:

> "Mientras los hombres viven sin ser controlados por un poder común que los mantenga atemorizados a todos, están en esa condición llamada guerra, guerra de cada hombre contra cada hombre. Pues la guerra no consiste solamente en batallas o en el acto de luchar, sino en un período en el que la voluntad de confrontación violenta es suficientemente declarada. (...) la naturaleza de la guerra no está en una batalla que de hecho tiene lugar, sino en una disposición a batallar durante todo el tiempo en que no haya garantías de que debe hacerse lo contrario. Todo otro tiempo es tiempo de paz.
>
> Por tanto, todas las consecuencias que se derivan de los tiempos de guerra, en los que cada hombre es enemigo de cada hombre, se derivan también de un tiempo en el que los hombres viven sin otra seguridad que no sea la que les procura su propia fuerza y su habilidad para conseguirla".

HOBBES contempla la necesidad de garantías para la paz y de una "fuerza" protectora ajena que proporcione seguridad y tranquilidad, pues esa será la forma de propiciar que el hombre deje su estado de naturaleza agresiva y pueda alcanzar una convivencia social pacífica. Es decir, se podrá lograr un "orden público" o social que permita tanto el desarrollo del grupo como el de los individuos que lo componen (como sujetos de deberes y derechos que pueden hacer uso de ellos de forma pacífica).

En conclusión, el Estado es la estructura que proporcionará el "orden público", pues será garante de los principios y valores de un momento social concreto, orientado a preservar el ejercicio de los derechos

[64] HOBBES, T. *Leviatán.* Ed. Alianza. Madrid, 1999. pp. 54 y 55.

fundamentales. Precisamente, decía Tribunal Supremo que (...) "el orden público en su aceptación de discurrir pacíficamente y sin alteraciones las instituciones públicas y privadas y la de los individuos en el ámbito de una comunidad, no puede oponerse al ejercicio de un derecho legítimo" (...)[65]. Y continúa razonando de forma que el "orden público" no puede ser causa de la limitación de derechos, pero sí de su ejercicio cuando acate para ello el ordenamiento jurídico, y se haga de forma que sea necesaria y proporcionada[66].

[65] STS de 20 de enero 1989 (F.Jº. 2º).
[66] En este sentido, otras sentencia de interés: STS de 27 de enero de 1987.

II. EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

1.– Contenido y alcance:

1.1.-Origen del Derecho: la protección de la libertad.

Se ha expuesto que la forma más adecuada de delimitar el contenido y alcance de los derechos humanos, debe partir de la definición de los requisitos necesarios para su efectiva realización, pues de lo contrario, nos encontraríamos ante meros "derechos de papel", que serían formulados careciendo de toda garantía y capacidad de tutela.

En concreto, para entender el alcance del "derecho fundamental a la protección de datos de carácter personal", de los llamados derechos de tercera generación, es preciso conocer la especial naturaleza de su origen.

El fundamento de los derechos humanos viene dado por elementos absolutos, objetivos y universales, propios del ser humano, tal y como ya se ha mencionado, y los pilares de su configuración se pueden concretar en reflexiones de corte iusnaturalista:

I.- La supervivencia y/o integridad física.

II.- La libertad.

III.- La igualdad.

A ello se añadía, con fundamento en reflexiones de corte realista, un segundo momento en su configuración. Se exigía como elemento imprescindible el "consenso universal". El acuerdo en la determinación de las necesidades más básicas del ser humano, va a sentar los cimientos para la compresión del alcance de los derechos humanos en un momento histórico, social y político concreto, en definitiva, los va a mostrar como ejercitables.

Percibidas las "necesidades humanas básicas" y, celebrado el "consenso universal" sobre su relevancia, el tercer momento a tener en cuenta para su total configuración no puede ser otro que la "previsión de su garantía". Esta tercera fase nos la brindaban las teorías de corte positivista con la exigencia de normalización de las previsiones determinadas por aquel consenso universal. Es necesario para determinar el alcance de un derecho, registrar la fórmula más apropiada para garantizarlo, para satisfacer las necesidades humanas y protegerlas de cualquier forma de amenaza. Podemos denominar la norma de muy distintas maneras en función del alcance de la eficacia protectora del derecho registrado en ella, ya sea Convenio, Declaración, Tratado, Constitución, etc., sin embargo, en todas ellas debe darse la seguridad de su ejercicio.

Ahora bien, dicho ejercicio nunca será efectivo si no se da otro elemento más en esa teoría. Si la "previsión de la garantía" no cuenta con un cuarto momento, de "concienciación social" sobre la fórmula adoptada para su protección y ejercicio, no podrá tenerse por materializada. Cuando

se observa la existencia de un derecho fundamental y se plantea la realización de su contenido en una comunidad de individuos, éstos no sólo deben haber llegado a un consenso sobre cuales son las necesidades que deben enmarcar, bajo el título "derechos", sino que además deberán aprender a convivir en una sociedad formada para su respeto. La "educación" de los miembros del grupo en las reglas de convivencia, es un paso imprescindible para que su individualidad, su personalidad y su dignidad como seres humanos, sean efectivas.

Por último, todos los elementos descritos para la configuración de los derechos fundamentales, una vez han sido determinados y dotados de contenido, hay que ponerlos en práctica, y eso implica sin excepciones, ponerlos en un espacio y un tiempo concretos. El quinto elemento sería definible a través de un único sustantivo: "evolución".

Una teoría sobre el fundamento de los derechos fundamentales con cinco elementos: "necesidades humanas básicas", "consenso universal", "previsión de su garantía", "concienciación social" y, "evolución". Un derecho fundamental sobre la que fijarla: el "derecho a la protección de datos de carácter personal". Y finalmente, un resultado práctico con las claves para la materialización de este derecho, y las consecuencias de sus propios límites.

El derecho a la protección de datos personales ha sufrido una evolución constante tanto en la determinación de su contenido como en la determinación de los conceptos que fundamentan su realización.

En un primer momento parecía surgir de una creación "ex novo" de la conciencia jurisprudencial del finales del Siglo XX, sin embargo, su realidad nace en primer lugar de la evolución del significado de la palabra "libertad" para el ser humano.

> LIBERTAD: "Facultad natural que tiene el hombre de obrar de una manera o de otra, y de no obrar, por lo que es responsable de sus actos"[67].

La propia Declaración de Derechos del Hombre y del Ciudadano de 1789, en el artículo 4, definía la libertad en los siguientes términos:

> "La libertad consiste en poder hacer todo lo que no daña a los demás. Así, el ejercicio de los derechos naturales de cada hombre no tiene más límites que los que aseguran a los demás miembros de la sociedad el goce de estos mismos derechos. Estos límites sólo pueden estar determinados por la Ley".

Se reconocía entonces expresamente el valor del que derivan los llamados derechos de la personalidad, el valor "libertad": "Los hombres nacen libres e iguales en derechos". Reflejo de dicha herencia lo son además las Constituciones contemporáneas que reconocen el derecho a la libertad como un derecho fundamental. En España, la Constitución de 1978, dice en su artículo 17.1:

> "Toda persona tiene derecho a la libertad y a la seguridad de su persona. Nadie puede ser privado de su libertad, sino con la observancia de lo establecido en este artículo y en los casos y en la forma prevista en la ley".

Toma la "libertad" como punto de partida para la efectiva consecución de la dignidad del ser humano, por el importantísimo papel que representa en general para el desarrollo de los llamados "derechos de la personalidad"[68]. Y fue entendida además[69] como el goce individual de determinadas facultades, bienes o poderes, en contra de lo que se entendía

[67] Diccionario de la Real Academia de la Lengua Española. Vigésima segunda edición.
[68] CONSTANT, B. *De la libertad de los antiguos comparada con la de los modernos*. Escritos Políticos, Centro de Estudios Constitucionales. Madrid, 1989. pp. 278 – 365.

antes: garantía política de participación en el poder de todos los miembros de la comunidad.

La libertad, como requisito previo para la efectiva realización de la personalidad del individuo, significa exigir una pieza más del derecho fundamental, el elemento "DIGNIDAD". Es decir, se precisa libertad para que el ser humano pueda emprender la realización de intereses individuales[70] con dignidad, aunque lo sea considerándola en el momento histórico que lo requiera.

La libertad es por tanto poder de decisión del individuo, y considerada en un Estado de Derecho, es además autonomía para decidir sin menoscabo de la integridad física ni moral, sólo limitados por la ley, frente a las amenazas del poder público y/o los demás individuos de la sociedad. Estado y sociedad son protectores, pero a su vez son potenciales amenazas para esa libertad, por cuanto pueden hacer variar su contenido y límites de realización, y de ahí su consideración tanto en su aspecto negativo (no injerencia estatal/social en la esfera individual), como en el positivo (garantía de acción, en cuanto a decidir cuándo y cómo puede permitirse una interacción entre la esfera estatal/social y la individual).

Las garantías de libertad y dignidad humana, o más bien, las fórmulas de su materialización en el discurrir de una vida en sociedad, han ido variando con el paso del tiempo: la libertad de pensamiento, de expresión, de religión, ideológica, de elección del lugar de residencia, etc. Si ponemos aquella primitiva "libertad", propia del intelecto, en relación directa con el particular entorno de un individuo cuya personalidad se desarrolla en la "Sociedad de la Información", podremos ver cómo se ha ido perfilando su naturaleza y contenido hasta llegar a lo que hoy conocemos como el "Derecho a la Protección de Datos", que no es un derecho nuevo, sino que es una nueva necesidad que requiere la "libertad" del individuo para su efectiva realización, al verse dañada por nuevas y distintas amenazas, como las que

[70] PEREZ LUÑO, P. *Derechos Humanos y Constitucionalismo ante el Tercer Milenio*. Ed. Marcial Pons. Madrid, 1996. p. 42.

implica precisamente el desarrollo de la "Sociedad de la Información", la tecnología y la informática.

Informática e intimidad comenzaron no hace mucho a mostrarnos el alcance y las posibilidades de otras amenazas, hasta ahora desconocidas, acotando concretas parcelas de libertad del individuo, y con ello, menoscabando su dignidad.

Precisamente, señala PABLO LUCAS MURILLO DE LA CUEVA que el origen de los derechos fundamentales, o en su reconocimiento, "es posible establecer una gradación de etapas o secuencias en las que juegan factores de distinta naturaleza. Ante todo, los de carácter material. Es decir, los que tienen que ver con una aspiración o necesidad individual cuya satisfacción se convierte en una exigencia tan imperiosa que llega a erigirse en condición indeclinable de la convivencia a partir de un momento dado en función de las relaciones sociales. En segundo lugar, la justificación ideológica de la pretensión de ver satisfecha esa necesidad básica y, en estrecha relación con ella, en tercer lugar, su reivindicación frente al poder público a través de distintas formas de acción y expresión. Por último, su declaración de manera más o menos solemne pero jurídicamente efectiva. Esos pasos, perceptibles en la génesis de los derechos de cualquiera de las generaciones de las que se viene hablando, se aprecian también en el caso del derecho a la protección de datos. El elemento determinante de la necesidad o interés esencial sobre el que se construye es el progreso tecnológico (…). Pues bien, en este contexto, la necesidad básica o interés vital a partir del cual surge la demanda de reconocimiento de un derecho es, precisamente, la de poner en manos de los interesados instrumentos que les permitan recuperar, al menos en parte, el control sobre la información personal que les concierne y que está o puede estar en manos de terceros. Esta pretensión se justifica a partir de la misma dignidad de la persona y guarda estrecha relación con la libertad que le caracteriza. Libertad individual entendida en su más amplio sentido, incluyendo la faceta de manifestarse o conducirse de acuerdo con la propia forma de ser"[71].

[71] LUCAS MURILLO DE LA CUEVA, P y PIÑAR MAÑAS, J.L. *Derecho a la autodeterminación informativa*. Ed. Fundación Coloquio Jurídico Europeo. Madrid, 1990. pp.14 y 16.

La protección de datos se estudia partiendo de la necesidad humana de proteger parcelas de libertad individual, en relación directa con la informática y las posibilidades que ofrece de recolección y tratamiento de información personal. En un primer momento la amenaza se empieza a analizar sobre el aspecto negativo y excluyente de la libertad, la "intimidad"[72], pero poco a poco se va poniendo de manifiesto que su garantía es mucho más amplia, puesto que la informática puede lesionar la libertad de un individuo para decidir sobre su propia información personal, aún no afectándole en "lo íntimo".

La necesidad de la protección de datos, se considera hoy independiente de los conceptos que en su momento la hicieron visible, la intimidad y la informática. Es un auténtico derecho autónomo e independiente, que determina la capacidad del individuo para decidir sobre su propia información personal.

1.2.- Contenido: la información personal.

El derecho a proteger la información personal, es hoy reconocido a nivel internacional como un derecho fundamental autónomo e independiente, cuyo contenido se ha ido concretando a lo largo de un complejo proceso evolutivo en el que confluyen tanto reflexiones doctrinales, como jurisprudenciales.

Las primeras manifestaciones de la necesidad de proteger esa parcela de libertad individual, surgieron de la observación de los efectos del progreso, en relación directa con la esfera de vida privada que los ciudadanos esperaban mantener reservada. Así, la noción de "intimidad"[73]

[72] Para los liberales, *"el disfrute de la libertad está intrínsecamente unido a la existencia de ese dominio privado que identifican con el marco de la realización humana".* BEJAR, H. El ámbito de lo íntimo. Ed. Alianza. Madrid, 1990. p. 34.

[73] "Intimidad": Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia*. Diccionario de la Real Academia de la Lengua Española*.

fue punto de partida de los planteamientos más reveladores sobre el alcance de la nueva necesidad y, en general, coincidían en que desde un punto de vista siempre negativo, este concepto se refiere a evitar toda intromisión de terceros en los ámbitos de la vida que su titular quiere reservar para sí. Podría definirse como:

> "aquellas manifestaciones de la personalidad individual o familiar, cuyo conocimiento o desarrollo quedan reservadas a su titular o sobre las que ejerce alguna forma de control cuando se ven implicados terceros, entendiendo por tales, tanto los particulares como los poderes públicos"[74].

Es evidente su condición de "derecho de la personalidad" y de expresión del valor de la dignidad humana, que debe ser respetado y protegido por un ordenamiento jurídico para permitir su efectivo ejercicio, pero el momento en que esto empezó a entenderse así, desde un punto de vista procesal, es difícil de precisar[75].

Hay un gran repertorio de doctrinas al respecto, que dependiendo del término que elijan para conceptuarlo, lo situarán en una u otra época, pero lo que lo cierto es que la primera formulación técnico–jurídica o jurídico–doctrinal que conocemos, surgió de manos de SAMUEL D. WARREN y LOUIS D. BRANDEIS. Ambos autores, influidos por las circunstancias políticas y sociales de su época (1890), y algunos problemas "de prensa rosa"[76], configuraron el marco jurídico de la privacidad[77] en su obra "The Right to Privacy". En ella se ordenaba este derecho como la garantía del individuo a la

---

[74] ROMEO CASABONA, C. M. *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la información*, prólogo de José Antonio Martín Pallín. Ed. Fundesco, Col. Impactos. Madrid, 1988. pp. 25 - 34.

[75] No es lugar éste para desarrollar toda una investigación sobre cuando el ser humano consideró necesario proteger su intimidad, ni debatir sobre lo que consideran relevante a estos efectos los "antiguos" o los "modernos" de BENJAMÍN CONSTANT, en su obra *De la libertad de los antiguos comparada con la de los modernos*, Escritos Políticos, Centro Estudios Constitucionales. Madrid, 1989.

[76] S.D.Warren estaba casado con la hija de un importante Senador de Boston, y quería mantener su vida privada al margen de los ojos de la prensa y evitar así escandalosas revelaciones sobre su díscolo "modus vivendi".

[77] "Privacy" o "right to be let alone", frase acuñada por el Juez estadounidense Cooley en su obra "*A Treatise on the Law of Torts*" de 1888, y basado en la frase popular inglesa "my home is my castle". El derecho a la propiedad comenzó a significar en un momento dado algo de mayor alcance que el mero hecho de ser titular de una propiedad física, significaba además a tener derecho de control exclusivo sobre lo que había o se hacía en su interior, siendo realmente expresión de la libertad para decidir en ese ámbito concreto: el castillo.

protección de su persona y, a su seguridad frente a cualquier invasión de su vida privada y doméstica. Se ocupaba de mencionar los problemas que suponía para ello la utilización de tecnologías, por ejemplo en la toma y difusión de imágenes de una persona sin su consentimiento. Se trataba por tanto de dar garantías y protección al ámbito de la vida personal y familiar que se desee mantener a salvo de toda injerencia ajena[78], al igual que la información personal que no deba salir del ámbito decidido por su titular como restringido. Ambos impulsaron la concepción de este derecho como fundamental dentro del ámbito de los "personalísimos", utilizando para ello el término anglosajón "privacy".

En Estados Unidos, a raíz de los trabajos de WARREN y BRANDEIS, muchos estudios y jurisprudencia continuaron su propuesta con el análisis del término "privacy", como el derecho de la inviolabilidad de la persona[79]. Cabe destacar las teorías de FRIED[80], quien estableció que la privacidad no implica sólo, la posibilidad de excluir a terceros de conocer lo relativo a uno mismo, sino también cualquier actuación de control sobre la propia información personal, todo ello a favor de preservar el ámbito personal "vida privada". El hecho de que otro conozca detalles personales de nosotros va a tener consecuencias sobre nuestra "privacy". Otro autor WESTIN[81], centró más su teoría en el derecho a controlar la información personal, concibiendo la "privacidad" como un instrumento para el objetivo de realización de todo ser humano, para su autodeterminación como persona ya sea considerada individualmente, ya lo sea dentro de un grupo. Es lo que se ha dado en llamar "Informational Privacy". En igual sentido, W. A. PARENT definió este término como la condición de no tener conocimiento de datos o información sobre terceras personas[82].

---

[78] Puede parecer un problema adaptar la intimidad así concebida a todos los periodos históricos que ha vivido la humanidad, pero no lo será si se entiende ésta como se ha venido señalando, como una manifestación más de la dignidad humana entendida en el momento histórico en que se esté analizando.

[79] WARREN SAMUEL, D. Y BRANDEIS, L. "The right to privacy". *Harvard Law Review*, Vol. IV, nº 5, 15 – XII –1890, p. 193 y ss. Traducción al español: *El derecho a la intimidad* (Benigno Pendas y Pilar Balsega ed.). Ed. Civitas. Madrid, 1995. p. 55.

[80] FRIED, C. Privacy, Yale Law Journal. Vol. 77. Connecticut, 1968. pp. 475-493.

[81] WESTIN, A.F. Privacy and Freedom. Atheneum. New York, 1967. pp. 173 y ss.

[82] *The Problem of Definition Privacy and Confidentiality.* From the U.S. Congress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information (OTA-TCT-576), Washington, DC., September 1993. Publised for the Charles Sturt University. Australia.
Se pueden consultar las citas de los autores reseñados en: http://www.csu.edu.au/learning/ncgr/gpi/odyssey/privacy/ota_pc.html

Desde la segunda mitad del S.XX, se han venido realizando extensos estudios sobre el alcance de los términos intimidad y privacidad, bien como conceptos distintos, bien como análogos, en cualquier caso, se trata de extraer lo que han ido aportando a la configuración actual de un concepto: "autodeterminación informativa". Lo que comenzó a desarrollarse alrededor del concepto "intimidad", se ha ido trasladando al territorio de la "privacidad", al entenderla como algo más amplio, que afecta a toda la información personal y no sólo a la íntima, pero siempre con la característica de excluir a terceros de su conocimiento. Se mantiene por tanto en la esfera de la vida privada, pero se reconocen las consecuencias que ello puede tener sobre las libertades de desarrollo de la persona, su esfera pública, de sociedad, como parte del Estado[83].

En España, la privacidad se ha definido en España como el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión"[84], de exclusión de terceros. Se utiliza siempre en un contexto negativo.

Las doctrinas de PÉREZ LUÑO y LUCAS MURILLO DE LA CUEVA, dos de las pioneras más destacadas (no las únicas), han contribuido enormemente a definir el alcance de éstos términos y también a ampliarlo teniendo en cuenta los avances sociológicos, históricos y tecnológicos, aunque no siempre coincidiendo en sus argumentos.

- FRIED, C. *Privacy*, Yale Law Journal. Vol. 77, Connecticut, 1968. "Privacy is not simply an absence of information about us in the minds of others, it is the control we have over information about ourselves. It is not simply control over the quantity of information abroad; it is the ability to modulate the quality of the knowledge as well".
- WESTIN, A. *Privacy and Freedom*, Atheneum, New York, 1967. "Privacy is an instrument for achieving individual goals of self realization, the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".
- *PARENT, W. A. Recent Work on the Conception of Privacy, American Philosophical Quarterly , VOI. 20, 1983.* "Privacy is a condition of not having undocumented personal information about oneself known by others".

[83] (...) "desde la obra de Warren y Brandeis, el concepto de derecho a la intimidad ha sufrido una importante variante, pues evoluciona de ser un simple derecho de exclusión en el que el individuo reafirmaba su derecho a la privacidad o "derecho a estar solo" para adquirir una nueva dimensión como derecho facultativo que le permite ejercer acciones en defensa de su vida privada". CASTRO BONILLA, A. La protección del derecho a la intimidad en el tratamiento de datos personales: el caso de España y la nueva legislación latinoamericana. *Revista Digital Alfa-Redi*, nº 111, Diciembre 2002. Se puede Disponible en http://www.alfa-redi.org/revista/revista.asp?idRevista=55

[84] Diccionario de la Real Academia de la Lengua Española.

PÉREZ LUÑO, señala que más que una pluralidad de conceptos con pluralidad de significados existe un concepto unitario de intimidad, basado en una textura abierta, plural, dinámica y globalizadora[85].

LUCAS MURILLO DE LA CUEVA dio un paso más allá, defendió que el concepto intimidad se puede distinguir incluso en dos fases propias de la Sociedad de la Información, la "preinformática" y la posterior, entendiendo esta segunda como más amplia y que abarca el control de la información personal que pueda afectar al ámbito privado[86]. Este autor introdujo cómo la cuestión tecnológica afecta a la conceptuación de los derechos fundamentales.

Por otra parte, RICARD MARTINEZ, establece "que existe una noción, la de vida privada o privacidad, que supera las limitaciones del término intimidad", es por tanto el término "vida privada" el que tiene esa mayor capacidad de alcance en su significado, superando los límites de la "intimidad" y entrando en todo lo que afecte a "información personal" susceptible de revelar aspectos privados del individuo. Recuerda también que debe tenerse en cuenta cómo, a través de ello, se pueden menoscabar otros derechos y libertades que afectan al libre desenvolvimiento de la personalidad en un marco de libertad. En este sentido, lo ve como un producto histórico y social que debe contemplarse en su dimensión tradicional como libertad negativa pero, también a la luz de su perfil positivo, como control sobre la información personal y, sobre todo, teniendo en cuenta cómo las nuevas tecnologías facilitan este tipo de revelaciones e intromisiones[87].

Y en opinión de JOSE LUIS PIÑAR, "el derecho a la privacidad es el derecho a la propia imagen, nombre y reputación; el derecho a controlar la información que se refiera a nosotros mismos, a la autodeterminación informativa, según el concepto acuñado por la doctrina alemana (…). La

[85] PÉREZ LUÑO, P. *Dilemas actuales de la protección de la intimidad*. Universidad Carlos III de Madrid. Madrid, 1994. pp. 311-338.
[86] LUCAS MURILLO DE LA CUEVA, P y PIÑAR MAÑAS, J.L. *Derecho a la autodeterminación …* Op. Cit. p. 98.
[87] MARTÍNEZ MARTÍNEZ, R. *Una aproximación crítica a la autodeterminación informativa*. Ed. Civitas. Madrid, 2005. pp. 35 - 44.

privacidad es, pues, condición indispensable para poder afirmar que una sociedad es democrática y respetuosa con los derechos fundamentales, pues sin ella, como acabo de decir, no puede hablarse ni de respeto a la dignidad ni de libertad"[88]. Comparte este autor, con STEFANO RODOTÁ[89], la idea de que "sin privacidad, tanto la dignidad como la libertad resultan sustancialmente afectadas hasta el extremo de poder, sencillamente, desaparecer o ser meramente testimoniales".

Cada paso, cada momento, ha significado un avance concreto en la comprensión del derecho a la intimidad, haciendo manifiesta la necesidad de incorporar nuevas garantías para proteger otros derechos y libertades que, a través de la conculcación indirecta de éste pueden verse menoscabados, y que en definitiva exceden de su alcance originario, como por ejemplo la libertad para decidir sobre uno mismo, su "modus vivendi" y el de su familia. En este sentido, el artículo 18.4 de la CE se centra en garantizar el libre desarrollo de la personalidad del individuo en su esfera privada, en la intimidad de su domicilio, de su familia y de sus comunicaciones, y además, lo haría respecto de una amenaza concreta: la informática.

Sin detenernos en pormenorizar la evolución de la Tecnología hasta lo que hoy ya conocemos como "Sociedad de la Información", es fácilmente identificable el punto en que las amenazas empiezan a materializarse para los derechos de los individuos a través de la informática. El riesgo surge en el momento en que comienzan a procesarse tratamientos automatizados de la información relativa a una persona, sobre sus características propias y perfil de personalidad, con medios y posibilidades en principio ilimitados (tanto en beneficios como en perjuicios). En ese momento surgen en el panorama internacional las nuevas teorías nuevas sobre la intimidad y sobre cómo protegerla de los ataques que se están produciendo (WARREN y BRANDEIS fueron, como se ha señalado, los pioneros en intentar delimitar estas circunstancias) en relación con todo ello.

---

[88] PIÑAR MAÑAS, J.L. ¿Existe la privacidad?, Inauguración Curso Académico 2008-2009. CEU Ediciones. Madrid, 2008. p. 21.

[89] STEFANO,R. *La vita e le regole. Tra diritto e non diritto*. Ed. Feltrinelli. Milán, 2006. pp. 103 y ss. Trad. *La vida y las reglas. Entre el derecho y el no derecho*. Ed. Trotta. Fundación Alfonso Martín Escudero. Madrid, 2010.

La tecnología hoy permite almacenar cantidades ingentes de datos sobre una persona y, las desarrolladas comunicaciones permiten enviarla en cuestión de segundos de un lugar a otro del mundo, para ser utilizados con finalidades no siempre conocidas, ni mucho menos lícitas. Todo ello significa que cualquiera puede tener información (privada o no) de una persona, y utilizarla para invadir su intimidad o coartar cualquiera otra de sus libertades[90].

El artículo 18.4 de la Constitución se ha encargado de señalar cómo se ha de dotar a las personas de la cobertura jurídica necesaria frente al peligro que supone la informática para la intimidad. Este párrafo cuarto dice que se debe hacer por Ley y, que además se garantizará "el pleno ejercicio de sus derechos", lo que significa que no sólo la intimidad está protegida frente a la amenaza "informática", sino que es más amplio, también lo están otros derechos y libertades de la persona. La Sentencia del Tribunal Constitucional 254/93 utilizó los términos "Libertad Informática" para referirse "al derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos".

Por todo lo expuesto, se puede afirmar ya que, siendo la libertad un derecho básico del ser humano (de primera generación) y la informática una nueva amenaza, propia de un momento histórico y social concreto (la Sociedad de la Información), el artículo 18.4 de la CE, es la respuesta clave para garantizar la realización o satisfacción de esa necesidad humana, frente a esa forma de amenaza. Esto es precisamente lo que se plantea con una conceptuación dinámica de los derechos fundamentales, un origen universal y una capacidad de adaptación flexible a los cambios.

La informática queda pues limitada en su uso por la Ley, por tanto, si la informática tiene como cometido principal tratar información, a estos efectos, la Constitución estará limitando el tratamiento de información. Es

[90] Conocer determinada información (pública o privada) de una persona no da derecho a utilizarla sin tener en cuenta su consentimiento para ello. Utilizarla de este modo, puede dar lugar a discriminaciones severas (por ejemplo, conocer la ideología política) y limitaciones a sus libertades en otros muchos aspectos (por ejemplo, conocer un domicilio posibilita llevar situaciones de acoso al extremo), que no siempre tendrán que ver con la esfera privada de su vida.

más, cuando la información es relativa a personas concretas, entonces estamos ante lo que en realidad debe tratar de proteger la Ley: el tratamiento automatizado de los datos de carácter personal. La información personal configura los perfiles individuales, dota a cada ser humano de una personalidad única e irrepetible, en definitiva de "individualidad".

Para entenderla dentro de la Sociedad de la Información, es imprescindible ponerla en relación con la informática y los ilimitados tratamientos de información que posibilita. Hasta no hace mucho, conocer determinados detalles de una persona estaba condicionado por espacios físicos no muy sencillos de traspasar, hoy, estos espacios se han ampliado a una esfera "virtual" donde el tratamiento y difusión de dichos detalles se han convertido en rutina, necesitan pues una especial protección, así, como ya hemos visto, el precepto que nos ocupa no sólo se limita a proteger el aspecto íntimo de los que definen la personalidad de un individuo, sino también el pleno ejercicio de cualesquiera otros derechos que igualmente se pudieran ver amenazados por este tipo de tratamientos. Se trata de proteger la libertad de decisión individual sobre la información personal (íntima y no íntima). Es posible pues ver superados los límites que marcaba la intimidad en la Constitución, reforzados por doctrina y jurisprudencia en la tarea de su protección. En el marco de las nuevas tecnologías y con su evolución imparable[91], la informática puede suponer una amenaza para todos los derechos y libertades de la persona, es decir, puede poner en peligro la dignidad de un individuo con el sólo tratamiento automatizado de su información personal.

[91] Según la llamada Ley Moore, por la que el 19 de abril de 1965, Gordon Moore, creador de Intel, señalaba en la Revista estadounidense Electronics Magazine, que la tecnología sufre una evolución constante y progresiva imparable, entendiendo que "los circuitos integrados llevarán a maravillas tales como ordenadores personales, o por lo menos terminales conectadas a un ordenador central, controles automáticos para los coches, y equipamiento de comunicaciones portátil personal", basándose en que La complejidad de los componentes se ha multiplicado aproximadamente por 2 cada año. A corto plazo, se puede esperar que esta tasa se mantenga, o incluso que aumente. A largo plazo, la tasa de aumento es un poco más incierta, aunque no hay razón para creer que no permanecerá constante por lo menos durante 10 años. Esto significa que para 1975, el número de componentes en cada circuito integrado de mínimo coste será de 65000. Creo que un circuito tan grande puede construirse en una sola oblea. Estas observaciones se consideran hoy día el motor del rápido cambio tecnológico". MOORE, G.E.. "Progress in digital integrated electronics", IEEE International Electron Devices Meeting, Vol. 21. IEDM Technical Digest 1975, pp. 11-13. Disponible en:
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=9941

El pleno ejercicio de derechos (intimidad o no) en relación con las amenazas de la informática, es clave para entender que el 18.4 de la CE no recoge un derecho de nueva creación, sino que, recoge la garantía de todos los derechos y libertades individuales en relación con una nueva amenaza.

Una vez vencido concepto "intimidad" como único fundamento del artículo 18.4 de la CE, y aún respetándolo, por cuanto mostró que existen determinadas necesidades del ser humano que no estaban cubiertas frente a nuevas amenazas, en la Sociedad de la Información debemos hacer una última reflexión sobre el concepto de "privacidad" que se ha tocado antes, para ver por qué se deja de lado desarrollar esta teoría.

Se ha dicho que la privacidad[92] abarca un área más amplia que la intimidad, que se refiere la información personal íntima y además al control de cualquier dato personal (también datos no íntimos), cuyo tratamiento pueda afectar a la vida privada. Esto es cierto, dilata el marco de interpretación para el artículo 18.4 de la CE, sale de lo íntimo pero, igualmente vuelve a quedarse paralizado en el círculo de la vida privada porque se dice siempre "en aquello que le afecte". Aunque inicialmente se reconocía que se pueda afectar otros derechos, finalmente acababa por reconducirlo a dicho círculo, incluso aun denominándola "informational privacy".

El control sobre la información personal no puede cerrarse en su origen al concepto de "intimidad", ni siquiera al de "privacidad" en su vertiente más estricta, porque lo que ha de garantizar se sale de su estricto ámbito inicial para alcanzar también lo no íntimo. Aun estando de acuerdo con parte de la concepción doctrinal señalada para esos términos, es necesario dar un paso más. Decidir sobre el uso y destino de los datos personales, se traduce por propia naturaleza en un poder de disposición sobre los mismos, en una libertad más para elegir cómo, cuando y dónde se quiere desarrollar la personalidad, ejercer otros derechos o ceder parcelas de cualquier índole respecto de la libertad.

[92] La "privacy" entendida por los Norteamericanos, y desarrollada para la Constitución Española por la doctrina. Cfr. MARTÍNEZ MARTINEZ, R. *Una aproximación crítica* … Op. Cit. pp. 254 - 300.

Teniendo fundamentado y claro el artículo 18.4 de la CE se refiere sin más a información personal del individuo (íntima o no) y, que se debe respetar en todo caso el "pleno ejercicio de sus derechos" (todos aquellos que se puedan ver afectados), se concluye que: "la ley ha de limitar el uso de la informática en el tratamiento de información personal". Es decir el ser humano tiene el derecho fundamental a controlar su información personal, todos los detalles de su individualidad, también respecto de otros derechos fundamentales y con ello, su propia dignidad. El artículo 18.4 de la CE garantiza todo esto frente a una amenaza concreta: la informática.

Este derecho ha sido llamado durante mucho tiempo "Derecho a la autodeterminación informativa" y, su ejercicio efectivo lo garantiza la disciplina llamada "protección de datos de carácter personal" que surge específicamente respecto de los tratamientos de la información personal a través de la informática. Precisamente la denominación de la garantía ha sido la que ha calado para referirse al derecho.

Expuesto lo anterior, aún queda una laguna por cubrir. Para superar el término "informática" como amenaza, se ha recorrido un largo camino que puede resolverse como una mera cuestión de tiempo. Es cierto que la informática nos abrió los ojos en lo relativo al tratamiento de información de carácter personal[93], y lo hizo sobre la esfera íntima de su titular, pero hoy ya hay que entender un derecho protegido tanto en relación con tratamientos automatizados como de tratamientos manuales[94]. Esta afirmación además lleva a deducir una máxima específica en esta teoría: cabría la defensa constitucional de la autodeterminación informativa sin tener que recurrir necesariamente al artículo 18.4 (bastaría acudir al artículo 10 como se mostrará más adelante).

---

[93] "La Libertad informática o autodeterminación informativa es la respuesta del presente al fenómeno de contaminación de las libertades - "Liberties Pollution"- (...) es un derecho que ha nacido con nosotros. Su génesis ha sido fruto del empeño legislativo, jurisprudencia, doctrinal y especialmente, cívico, de quienes se afanan por ofrecer una adecuada réplica al desafío del tiempo tecnológico, que identifica nuestras formas de existencia". LOSANO, M. G., PERÉZ LUÑO, P. y GUERRERO MATEUS, M. F. Libertad informática y Leyes de protección de datos personales. Centro de Estudios Constitucionales. Madrid, 1989. p. 162.

[94] Disposición Adicional primera de la LOPD. Ficheros preexistentes: "En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados". Este plazo se cumple en el año 2007. Tal vez el artículo 10 CE sea el complemento perfecto para entender lo que depara el 2007 a estos efectos.

1.3.- El bien jurídicamente protegido: el derecho a decidir.

Durante mucho tiempo se consideró un amplio sector de la doctrina[95] consideró sinónimos el "derecho a la libertad informática", el "derecho fundamental a la autodeterminación informativa" y el "derecho a la protección de datos de carácter personal", pero hay diferencias prácticas que deben tenerse en cuenta. El primero, alude al bien jurídico que hay que proteger con la garantía del artículo 18.4 de la CE (protección de la libertad individual, en el entorno informático); el segundo, alude al derecho cuyo contenido define la jurisprudencia constitucional y, se debe entender como parte de la previsión del artículo 10.1 de la CE[96]; y el tercero aludiría a la garantía de protección. A pesar de ello, se entiende que "protección de datos" es el término utilizado habitualmente para referirse a todas las implicaciones que se vienen tratando sobre este derecho fundamental.

Se ha planteado hasta una teoría sobre el fundamento del derecho a la protección de datos que implica tanto al artículo 10 de la CE como al artículo 18 de la misma norma. El primero, relativo a la dignidad del ser humano, abre la puerta al segundo, a la capacidad de decidir sobre la propia información personal, como una facultad inherente al desarrollo personal digno del ser humano y al que, en consecuencia, se debe dotar de las garantías y protección propias de los derechos humanos.

La intimidad concebida simplemente como un elemento de exclusión, se ha cuestionado por autores como PÉREZ LUÑO, que señala que, junto a la noción de dignidad, debe tenerse en cuenta el punto de vista "positivo" para el momento de llevarlo a la práctica, para poder establecer los medios que

---

[95] BAÓN RAMÍREZ, R. "Visión general de la informática en el nuevo Código Penal". *Revista del Consejo General del Poder Judicial. Nº XI, Ámbito jurídico de las tecnologías de la información*. Madrid, 1996; ORTI VALLEJO. A. *Derecho a la intimidad informática*. Ed. Comares. Granada, 1994; LOPEZ DIAZ, E. El derecho al honor y el derecho a la intimidad. Ed. Dikynson. Madrid, 1996. Entre otros.

[96] Artículo 10.1 CE. "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 son fundamento del orden político y de la paz social".

permitan su efectivo ejercicio. La protección de datos de carácter personal en la práctica significa capacidad de decisión tanto sobre esa parte privada como otro tipo de información personal[97]. Por tanto, es importante distinguir y hablar de dos derechos[98] independientes, intimidad y protección de datos, que interactúan desde el individuo y hacia su desarrollo en sociedad[99]. Aunque que ambos implican aspectos positivos y negativos de un derecho fundamental, lo es del derecho a la libertad, como parte esencial de la dignidad del ser humano (artículo 10 de la CE). Es decir, hay que considerar la libertad para decidir desde que es manifestada en la esfera del intelecto, libertad para decidir, y hasta que es proyectada en la sociedad. Esta proyección se declara en su vertiente negativa (intimidad) como la decisión de excluir a terceros de la esfera personal o privada y, en su vertiente positiva (autodeterminación informativa) como la decisión de hacer partícipes a terceros de la información personal.

Ahora bien, la evolución sufrida por estos conceptos, ante la aparición de la informática y sus posibilidades para el tratamiento de la información de carácter personal, han resultado en una nueva perspectiva de garantía con el artículo 18.4 de la Constitución. Es notorio como la doctrina primero, y la jurisprudencia después, han ido llenando de contenido este precepto, hasta llegar a la protección que ofrece la legislación vigente en España (Ley Orgánica 15/99 de Protección de Datos de Carácter Personal) y cuya denominación es la utilizada comúnmente para designar hoy la capacidad para decidir libremente sobre la información personal.

---

[97] No significa lo mismo, poder decidir sobre el aspecto negativo (no injerencia de terceros en aspectos de la intimidad, en informaciones de la vida privada), que sobre el aspecto positivo (decidir cómo y cuándo sobre la difusión de la información personal), al igual que no implica lo mismo, el derecho a la inviolabilidad del domicilio (de la esfera de la intimidad), que el derecho a decidir quién quiero que entre en mi casa (esto se enmarcaría de forma más adecuada en los derechos de propiedad).

[98] Se trata de intimidad y autodeterminación informativa, y no se refiere tanto a "derecho" como a "exigencias y garantía de protección". Se utiliza para denominarlos "derechos" para simplificar la exposición.

[99] (...) "en nuestra época resulta insuficiente concebir la intimidad como un derecho garantista (status negativo) de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla, al propio tiempo, como un derecho activo de control (status positivo) sobre el flujo de informaciones que afectan a cada sujeto. Esta ampliación del contenido de la intimidad ha tenido puntual repercusión (...) así en nuestros días (...) junto a su conexión con la dignidad, se identifica la intimidad con la propia noción de la libertad, en cuanto define las posibilidades reales de autonomía y de participación en la sociedad contemporánea" (...). PEREZ LUÑO, P. *Derechos Humanos, Estado de Derecho y Constitución*. Ed. Tecnos. Madrid, 1984. p. 330.

La comisión CALCUTT explica que es "el derecho del individuo a que se le proteja de la intromisión, ya sea mediante medios físicos directos o mediante la publicación de una información, en su vida personal o en sus asuntos personales o en la vida o asuntos personales de su familia"[100].

Uno de los conceptos mencionados, y que ha marcado el debate en torno al que se vienen desarrollando los anteriores apartados, es el de "libertad informática". Tal vez sea que, a efectos prácticos, puede mostrar en dos palabras el origen y razón de ser del artículo 18.4 de la CE desde el mismo año 1978. La STC 254/1993 declaró sobre este precepto que "incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona. Además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizo de datos" (F.J. 6º). Esta sentencia fija claramente el amplio espectro práctico del artículo 18.4 de la CE, sin embargo después lo reduce a la esfera de la intimidad y su relación con la informática, diciendo en su F.Jº. 7º que "la garantía de la intimidad lato sensu, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".

En todo caso, en estos dos significativos párrafos, el Tribunal Constitucional logra transmitir el momento que se está queriendo garantizar, el verdadero alcance que debe tener el derecho a decidir libremente la protección de datos. Se citan las libertades individuales y la dignidad como punto de partida, la intimidad como bien jurídico concreto amenazado, y la informática como la amenaza a combatir. Para ordenar todo esto en el marco

[100] COMISIÓN CALCUTT: "Informe sobre la intimidad y cuestiones afines". *Cuadernos del Consejo General del Poder Judicial*. Trad. de M.E. Sánchez Suárez. Madrid, 1991. p. 27.

constitucional, amplía el alcance del derecho a la intimidad tanto sobre lo íntimo como sobre lo no íntimo. Hay que decir que como sentencia, esta resolución es de obligada referencia para la interpretación del artículo 18.4 de la CE, puesto que impuso los elementos que lo caracterizarían hasta su final conceptuación, aunque eso si, hilándolos de manera discutible como se ha señalado y, como se verá más adelante en el análisis de la jurisprudencia constitucional habida en España en esta materia.

Pues bien, en nuestro panorama jurídico la "libertad informática", exige las libertades individuales en un espacio nuevo en el que domina la informática (el espacio virtual), siguiendo la estela del derecho a la intimidad, para acabar centrándose en el de la autodeterminación informativa. La consecuencia práctica es sin duda la protección efectiva de un derecho autónomo e independiente del derecho a la intimidad, que tiene su origen en la libertad individual para decidir sobre uno mismo y la información que nos individualiza, que se puede denominar como "derecho de autodeterminación informativa" y que se ha garantizado a través del "derecho a la protección de datos personales". Que además, aun habiéndose manifestado a través de los avances tecnológicos y su repercusión sobre el derecho a la intimidad, e incluso otros derechos y/o libertades[101], en realidad constituye una más de las libertades del ser humano. Es decir, ha de quedar definitivamente superada en el panorama constitucional su dependencia del derecho a la intimidad y al ámbito virtual.

[101] La STC 11/1998, de 13 de Enero, sobre el carácter instrumental de la libertad informática. "En relación con la revelación de datos de carácter personal sobre la ideología y afiliación sindical, datos considerados como especialmente protegidos, y su repercusión en la libertad sindical del afectado. Se pone en relación un derecho de primera generación (libertad) con su manifestación progresista de segunda generación (libertad sindical), que finalmente, se configura como un derecho de tercera generación (derecho a la protección de datos). Esta sentencia lo denomina un derecho de carácter instrumental: Establecidas estas consideraciones con relación a la libertad sindical (artículo 28.1 CE), y a la protección de los datos informáticos (artículo 18.4 CE), es procedente desde la perspectiva constitucional situar correctamente la relación de los citados arts. 18.4 y 28.1, respecto de la libertad sindical. En efecto, el artículo 18.4 en su último inciso establece las limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos, lo que significa que, en supuestos como el presente, el artículo citado es, por así decirlo, un derecho instrumental ordenado a la protección de otros derechos fundamentales, entre los que se encuentra, desde luego, la libertad sindical, (...) En suma, ha de concluirse que tuvo lugar una lesión del artículo 28.1 en conexión con el artículo 18.4 CE. Este no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona, la privacidad según la expresión utilizada en la E. de M". de la LORTAD, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios. Y aquí se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio del derecho de libertad sindical.

Pero no debemos dejar de lado el hecho de que, si bien el artículo 18.4 de la CE es el marco perfecto para instrumentar la protección de los derechos y libertades ante la grave amenaza que puede suponer la informática al tratamiento de la información personal, cuando nos encontremos fuera de este espacio, deberá acudirse al artículo 10 de la CE, que sostiene que "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 son fundamento del orden político y de la paz social. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España".

Más aún, si bien es cierto que, "si como parece desprenderse de la argumentación de nuestros constituyentes, se deseaba extender la garantía frente a los abusos informáticos, no sólo al honor y la intimidad, sino a todos los derechos fundamentales, hubiera sido preferible dedicar por entero un artículo entero de la Constitución"[102], la particularidad de que el derecho la protección de datos esté inserto en el marco del artículo 18 de la CE no puede entenderse en ningún caso como subrogado a su núcleo esencial ni tampoco, desde un extremo opuesto, defenderse su autonomía dogmática en el sentido de una declaración de aislamiento del resto de derechos. Los derechos fundamentales son interdependientes, se apoyan los unos en los otros reforzándose recíprocamente. El derecho a la protección de datos personales, así como el resto, está relacionado directamente con la dignidad humana y el libre desarrollo de la personalidad. De hecho, el propio artículo 18.4 hace referencia al ese "ejercicio de otros derechos" de la persona y es que, libertad sindical, propia imagen, libertad religiosa, honor, etc., pueden ser lesionados por un tratamiento incorrecto de los datos personales del individuo[103].

[102] "Informática y libertad: Comentario al artículo 18.4 de la Constitución", *Revista de estudios políticos*, Nº 24. Madrid, 1981. p. 44.
[103] GUERRRERO PICÓ, Mª C. El impacto de internet en el derecho fundamental a la protección de datos de carácter personal. Ed. Aranzadi, S.A. Navarra, 2006. pp. 204 y 205.

Sea cual sea el camino interpretativo que se tome el resultado es el mismo, se quiere proteger la información de carácter personal y, sobre todo, la capacidad de disposición que sobre ella tiene su titular.

En Europa, la primera sentencia de un Tribunal Constitucional que hacía referencia a la protección de datos personales fue la alemana, dictada 1983, sobre la Ley del Censo. Esta Sentencia versaba sobre la posibilidad de que el Estado utilizase datos de carácter personal de los ciudadanos para finalidades distintas de aquellas para las que fueron recabados sin su consentimiento. Configuró en ese momento el antecedente para toda Europa sobre lo que debía entenderse como tratamientos de información o datos de carácter personal, y lo llamó. "el derecho a la autodeterminación informativa", términos que reflejan perfectamente a qué capacidad individual se refiere esta exposición, y lo que en esencia debe ser garantizado para su efectivo ejercicio.

Una definición:

> "Denominamos autodeterminación informativa a la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los tratados mediante medios informáticos"[104].

Esta definición muestra con una sencilla redacción su esencia ("control sobre información personal") sin olvidar su especial "origen" o amenaza ("medios informáticos"). Tratando de dar luz al contenido de un derecho concreto, autónomo e independiente, se ha venido mostrando que, a pesar de que se ha manifestado a través del derecho a la intimidad y respecto de determinadas circunstancias sociales (nuevas tecnologías), no es de éste del que se ha de partir para determinar su contenido fundamental, sino con el que tan sólo ha de compartir un origen común.

[104] CHRISTIAN HESS, A. "Derecho a la intimidad y autodeterminación informativa". Artículo publicado en la revista electrónica del proyecto *Democracia Digital.* Enero, 2002. Disponible en: http://www.democraciadigital.org.

Se trata de permitir el ejercicio efectivo de un derecho más de entre los derechos y libertades del hombre, protegiéndolo de amenazas reales y, permitiendo así el libre desarrollo de su personalidad en sociedad, pues de ello dependerá que lo estén otras muchas libertades conexas (libertad de expresión, de ideología, sexual, de religión, de movimiento, etc.).

Por último, siguiendo la línea de los acuerdos internacionales sobre derechos humanos citados, hay que mencionar la Carta de los Derechos Fundamentales de la Unión Europea, proclamada en el año 2000 en Niza, cuyo artículo 8 dice: Protección de datos de carácter personal.

> "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

Como se puede apreciar, el término "informática" o "tratamientos automatizados" ya no aparece, se ha superado y por tanto sirve como ejemplo perfecto de lo que se propone acreditar en esta exposición. Se ha comentado también que la tarea de Tribunal Constitucional para darle forma a este derecho fundamental, desde la redacción del artículo 18.4 de la CE, surgió como respuesta a la necesidad[105] de contrarrestar la fuerza de un ataque a las libertades sociales que iba cambiando muy rápidamente, de hecho, pocos años después de su primera formulación fue necesario revisar su conceptuación para superar viejas fórmulas y continuar dando respuesta a necesidades de garantía mucho más amplias[106].

---

[105] STC 254/1993 Op. Cit.

[106] Por su parte, la STC 254/1993 declaró con relación al artículo 18.4 C.E., que dicho precepto incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los

1.4.- Concepto práctico de la "Protección de datos".

Hasta ahora se ha puesto de manifiesto que se garantiza la libertad del individuo, frente a la informática, a través del artículo 18.4 de la CE: (...) "la Ley limitará el uso de la informática"[107], y ello por razón del especial peligro y consecuencias que aquella puede suponer para las libertades y derechos del individuo, en especial para su intimidad. Además, esta garantía, así entendida, se ha desarrollado respecto de los tratamientos de información de carácter personal[108], a través de una Ley Orgánica que pretendió adaptarse a la evolución e implicaciones de la sociedad de las Tecnologías de la Información y las Comunicaciones (TIC). Surgía así en España la LO 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), predecesora de la actual Ley 15/1999 de Protección de Datos de Carácter Personal (LOPD), para la defensa del derecho de las personas a "controlar el uso que se haga de su información personal inserta en un programa informático (habeas data)" según establece la STC 254/93 en su F.Jº. 7º. La garantía del "habeas data", lo es sobre un objeto concreto: la información personal, los datos de carácter personal. Protegiendo los datos que identifican a las personas, se protege a éstas y, por tanto, es necesario entender o definir su alcance práctico.

El Grupo de Trabajo creado por el Artículo 29 de la Directiva 95/46/CE, es una entidad independiente en Europa, encargada de investigar

---

derechos de la persona. Además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos (F.Jº. 6º). La garantía de la intimidad, latu sensu, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (F.Jº. 7º). STC 11/1998 (F.Jº. 4º)

[107] STC 292/2000 (F.Jº. 4º). ''Ahora bien, con la inclusión del vigente artículo 18.4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona"(STC 254/1993, de 20 de julio, F.Jº. 6º)".

[108] El tratamiento de información es en concreto el punto débil para las libertades en el ámbito informático.

y dar opinión a la Comisión Europea en la específica materia que nos ocupa. Entre sus múltiples trabajos, está la Opinión 4/2007 sobre el concepto de "dato personal", que fue adoptado con fecha 20 de Junio de 2007, para ofrecer una información clave en la definición del objeto de garantía. Llama la atención que dicho grupo de trabajo, optase por emitir este informe sobre las bases del derecho a la protección de datos, cuando la concienciación social e institucional sobre su importancia, debería estar ya muy avanzada e incluso consolidada.

Comienza el informe refiriéndose a la redacción que la Directiva 95/46/CE da a la definición de dato personal, destacando que significa: "cualquier información relativa a una persona natural identificada o identificable". Se trata de una definición muy general, tanto como fue posible, para incluir toda la información concerniente a un individuo identificable, sin embargo, la propia Directiva contiene después los límites que deben guiarla en su aplicación práctica, así, centra la cuestión en el equilibrio que debe existir entre la protección de datos personales y lo intereses legítimos de quienes los controlan o los tratan[109]. Entiende el Grupo de Trabajo del Artículo 29 que el hecho de querer limitar el fácil acceso que permite la tecnología, a los datos personales, no debe implicar una restricción tal de su tratamiento, que impida el legítimo ejercicio de los derechos de terceros.

Este informe analiza el contenido del concepto "datos personales" partiendo de sus cuatro elementos principales:

a) "cualquier información"
b) "relativa a"
c) "persona natural"
d) "identificada o identificable"

El primero de ellos contiene por su naturaleza otros dos elementos esenciales, uno objetivo y uno subjetivo, configurados por los datos que

[109] Por ejemplo, los artículos 10.c., 11.1.c. ó 18 de la Directiva 95/46/CE.

objetivamente describen a la persona y por los que, subjetivamente, terceras personas la identifican. Todo ello puede ofrecer información relativa a la intimidad del sujeto en cuestión, relativa a su identificación en sociedad, relativa a su relación laboral y económica con ésta, etc. Si bien es cierto que el ámbito más reservado de la persona es el que afecta a su vida privada, no lo es menos que la Carta de Derechos Fundamentales de la Unión Europea recoge el derecho a la protección de datos en su artículo 8, como un derecho autónomo, separado y diferente de la vida privada (artículo 7), para proteger los derechos y libertades de una persona y, en particular (pero no en exclusiva) su derecho a la privacidad.

Otra de las particularidades de este informe, sobre concepto de dato personal, es que no estima necesario que la información esté contenida en una base de datos estructurada o fichero. También la información contenida en el texto libre de un documento electrónico puede calificarse como dato personal y, por tanto, debe ser protegida de conformidad con la garantía que se establece para ello.

Respecto del elemento "relativo a", el Grupo de Trabajo del Artículo 29, señala que se refiere a "que versa sobre una persona". En este aspecto, reconoce además que en ocasiones es difícil determinar si los datos conciernen a personas o a objetos, es decir, distinguir si los datos personales afectan a la persona sólo de forma indirecta (por ejemplo el valor de una casa o la matrícula de un vehículo). Señala al respecto que dicha información deberá ser tratada como "dato personal" siempre que los datos se refieran al individuo, de forma que se refieran bien directamente a su identidad, bien que lo haga indirectamente, siempre u cuando permita evaluar sus particularidades y comportamiento en sociedad.

El elemento "identificado o identificable", en esta propuesta de contenido para el derecho a la protección de datos, es matizado en el sentido de que una persona estará identificada cuando, respecto de un grupo de individuos, es distinguible de los demás y, también cuando, aun no estando identificado, sea posible identificarlo. En este punto retoma el problema de la identificación directa o indirecta, para insistir en que cuando

es no posible poner por sí solos una serie de identificadores, en relación con una persona concreta, y sin embargo si lo es cuando se evalúan en conjunto, sólo podrán ser considerados datos personales cuando esté siendo tratados en conjunto y no, individualizadamente. Señala como ejemplo que, el nombre de una persona si es un identificador pero, por si solo, no puede identificar a una persona. Necesita más detalles de ésta, o bien, tratarse de un proceso muy limitado en número de personas y nombres muy característicos. Pone de relieve este informe que, la posibilidad de identificar a una persona va a depender, no sólo de los identificadores, sino también de su tratamiento y de quienes lo realizan, es decir, si son capaces de individualizar a una persona con la información de que disponen y la tecnología a su alcance, de una forma razonable.

Otro aspecto importante a tener en cuenta es precisamente cuando la finalidad del tratamiento de datos no es la de identificar a alguien, y así, repasa el informe algunas situaciones particulares como el uso de datos codificados, pseudónimos, o datos anonimizados.

Los pseudónimos son utilizados para recabar datos personales de un individuo sin dar a conocer su identidad real. Su efectividad va a depender de diferentes circunstancias, es decir, si se puede descubrir quién es el individuo a quien corresponde el pseudónimo. Generalmente estas circunstancias van a depender del volumen de pseudónimos y perfiles, del volumen de datos que compongan los perfiles y, de las medidas de seguridad que existan para impedir la identificación. Por ejemplo, los códigos o claves asignados a identificadores comunes (nombre, dirección, fecha de nacimiento., et) que se guarden separados. Por otra parte, aunque en idéntico sentido, los datos codificados, harán depender su eficacia de que éstos y las claves existentes para decodificarlos, sean almacenados separadamente. Respecto de los datos anonimizados, el informe del Grupo de Trabajo del Artículo 29, señala se diferencia de los anteriores en que por naturaleza no permiten la identificación de una persona, de tal forma que no dependen de ninguna circunstancia ajena y son usados sin estar en relación con un individuo. Podría darse el caso de que configuraran un "dato personal" en el sentido que indica el informe, si se guardan pocos datos y

además, se hace respecto de circunstancias muy delimitadas (por ejemplo, datos estadísticos de una comunidad de vecinos compuesta por cuatro viviendas).

El cuarto elemento de la definición, la persona. Ésta es el objeto esencial de protección, por tanto, los sistemas de procesamiento de datos (tratamientos automatizados), deben ser utilizados al servicio del hombre y, deben por tanto respetar sus derechos fundamentales y libertades, cualesquiera que sea su nacionalidad o residencia.

Se da en este punto un supuesto especial, el de las personas fallecidas. La Directiva 95/46/CE no ampara estos supuestos, pero, deben igualmente ser considerados dignos de protección si se encuentran bajo determinadas circunstancias, por ejemplo, cuando no exista constancia cierta del fallecimiento de la misma, el tratamiento de los datos debe hacerse como si de un ausente vivo se tratase (también los sería, de conformidad con el Código Civil español). También habría de procurar dicho respeto cuando por ejemplo, la información de la persona fallecida afecta a personas vivas, como puede hacerlo la información sobre una enfermedad hereditaria, aunque, en este caso, otras normas entrarían en juego para proteger a la persona, como son el deber del secreto médico, el derecho a la intimidad familiar.

En relación con este supuesto especial, el informe de referencia trae a consideración el caso de los "no-natos", que está sujeto a las normativas específicas de cada Estado de la Unión Europea sobre el reconocimiento que se otorgue a esta particular situación y, también, a la de los embriones, especialmente en lo que se refiere a los derechos hereditarios o al tratamiento de la información genética de los embriones.

Por último, las personas jurídicas. La Directiva 95/46/CE, consciente de que es un supuesto ajeno a la protección de datos que regula, habla sin embargo de la protección de los intereses legítimos de las personas jurídicas, bien en el caso en que la denominación de la misma fuese, por propia naturaleza, un dato personal (por ejemplo "Hnos. Alonso Martín,

S.L."), bien en el caso del Spam. Este último es el más controvertido y, los Estados miembros de la UE deben delimitar su alcance y protección de conformidad con la normativa europea[110].

Como conclusiones, lo resume en cuatro puntos relativos a los cuatro elementos citados. La necesidad de su garantía viene dada pues por sus propias nociones:

1º "Cualquier información": Se señala la voluntad del legislador europeo de diseñar un concepto amplio de dato personal, independiente de la naturaleza, del contenido de la información o del formato técnico en que ésta se presente. Tanto la información objetiva como subjetiva de cualquier conjunto, sobre una persona, puede ser considerado dato personal.

2º "Relativo a": este elemento juega un papel crucial en la determinación del alcance sustantivo del concepto, especialmente en relación con determinados objetos y las nuevas tecnologías. La Opinión da tres elementos alternativos (contenido, finalidad y resultado) para determinar si la información es "relativa a" un individuo o no. También señala así comprendida la información que pueda tener un impacto claro en la forma en que una persona es evaluada o tratada

3º "Identificado o identificable": se centra en las condiciones en que un individuo debería ser considerado "identificable" y, especialmente en la expresión "por el empleo de medios razonables" en relación con los medios que han de poder utilizarse para identificar a una persona física, ya sea por el responsable del tratamiento o un tercero.

4º "Persona física": Los datos personales han de hacer referencia en todo caso a personas vivas. Se tratan como especiales los casos de los fallecidos, los no-natos y las personas jurídicas.

[110] Artículos 1.2 y 13.5 de la Directiva 95/46/CE.

Establece en definitiva que las reglas de protección de datos están diseñadas para proteger todas aquellas situaciones en los derechos individuales pueden estar en riesgo, a través del tratamiento de la información que nos caracteriza.

2. Reconocimiento normativo:

2.1. – Antecedentes en España.

Desde la perspectiva de la tradición, el reconocimiento de Derechos Fundamentales en España se ha ido plasmando en normas de rango superior que no está de más reseñar, hacer un breve recorrido por algunos de los hitos más importantes del reconocimiento constitucional de la garantía de la protección de datos, partiendo del derecho a la dignidad, enmarcándolo en el contexto del derecho a la intimidad, y conceptuándolo de forma autónoma a través del artículo 18.4 de la CE.

Históricamente, el reconocimiento de la individualidad del ser humano y la necesidad de ordenar su pacífica convivencia tiene una de sus primeras manifestaciones en España en la Carta Magna Leonesa[111], otorgada por Alfonso IX (1171-1230) cuando accede al trono en 1188. Contenía una primitiva mención (o catálogo) de derechos individuales como la alusión al derecho a la inviolabilidad de domicilio o el derecho a la propiedad privada (apdo. 9º)[112]:

> "También juré que ni yo ni nadie entre en la casa de otro por la fuerza, ni haga ningún daño en ella o su heredad".

[111] SÁNCHEZ – ARCILLA BERNAL, J. "La obra legislativa de Alfonso X el sabio". *Revista general de legislación y jurisprudencia III*. Nº 1. Marzo, 2003. p.107 – 135.
[112] ALBACAR LÓPEZ, J.L. *Protección de los derechos fundamentales en la Nueva Constitución Española*. Ed. Panorama, Madrid, 1978. p. 22.

También, la Pragmática de los Reyes Católicos de 1490 mencionaba la libertad de residencia de los ciudadanos y el respeto a la esfera privada del domicilio[113], y más concreta sobre el derecho a la intimidad, una Real Cédula del Rey Felipe II[114], de 1592, en la que se reconoce de manera expresa la inviolabilidad del domicilio y de la correspondencia.

Pero no será hasta el S.XIX, que la conciencia social estimó necesario proteger la libertad individual frente a injerencias de terceros, y le dio relevancia constitucional como un derecho subjetivo, con las diferencias propias de cada etapa social y política[115], considerándose diferente relevancia de los mismos, y distintas prioridades sobre su protección.

En 1808, la Constitución de Bayona[116], otorgada por Napoleón, centraba su preocupación en el establecimiento de un orden político (la Corona, Consejo de Estado, Ministros y Senadores), judicial, territorial (Reinos) y religioso estables, pero también se reconocieron como derechos individuales dignos de especial protección, la inviolabilidad del domicilio (artículos 126) o la seguridad personal (artículos 127 y siguientes).

Con la Constitución de 1812 ("La Pepa")[117], promulgada el 19 de Marzo en Cádiz, aún no se podía hablar de una declaración completa y ordenada de derechos, pero lo es cierto que reconoció importantes derechos subjetivos de naturaleza liberal, tales como la ciudadanía española, la propiedad privada, la seguridad personal, las libertades de expresión e imprenta, la libertad de industria, la el derecho al arbitraje, etc. Y, como no, también tuvo en cuenta la inviolabilidad de domicilio. Esta tendencia progresista - liberal de reconocimiento de derechos de los individuos, fue heredada por la mayor parte de las constituciones que le sucedieron en la ordenación de la política, económica y social del territorio español. Así, la Constitución de 1837, que introdujo por primera vez una carta de derechos y

[113] SUAREZ FERNÁNDEZ, L. *La pragmática de Alcalá en la Política de los Reyes Católicos*. En Anales de la Academia Matritense del Notariado. T. 43. Ed. Edersa. Madrid, 2006. pp. 519 – 522.
[114] GARCÍA CUADRADO, A. *Derecho, Estado y Constitución. El Estatuto científico y otros temas fundamentales de derecho constitucional.* Editorial Club Universitario. Alicante, 2010. p. 321.
[115] CARMONA Y CHOUSSAT, J.F. *Constituciones: interpretación histórica y sentimiento constitucional. Cuatro ensayos sobre la organización política.* Ed. Thomson – Civitas. Navarra, 2004. pp.43 y ss.
[116] Texto disponible en: http://cadiz2012.universia.es/pdf/doc_0006_cons_1808.pdf
[117] Texto disponible en: http://www.congreso.es/constitucion/ficheros/historicas/cons_1812.pdf

libertades ordenada y homogénea[118]; o la Constitución liberal-democrática de 1869[119], preveía un título propio, el Título I: "De los españoles y sus derechos". La Constitución de 1931, por su parte, supuso un novedoso avance en esta línea, por cuanto en su Título II reconocía los derechos fundamentales de la tercera generación o derechos sociales y económicos, junto a los derechos políticos y civiles clásicos de las anteriores constituciones liberales. Además, quiso fortalecer sus garantías con la creación de un "Tribunal de Garantías Constitucionales", que tenía reconocidas entre otras, la potestad de conocer de los recursos de amparo en materia de derechos fundamentales.

Por el contrario, las constituciones más conservadoras, como la de 1845[120] y la de 1876[121], se mostraron más preocupadas por realzar la posición de la Corona, y por instaurar un equilibrio entre el radicalismos revolucionarios y conservadurismos propios del Antiguo Régimen, que por continuar desarrollando los derechos de los ciudadanos, pero sin llegar al extremo alcanzado en 1938, con el "Fuero del Trabajo" o, en 1945, con el "Fuero de los Españoles"[122], cuyo reconocimiento de derechos y libertades públicas para el ciudadano era puramente simbólico, puesto que no habían sido elaboradas ni aprobadas por representantes populares[123].

Por último, en 1978 nace la actual Constitución Española, de naturaleza progresista, que se establece un orden prioritario en la protección de los valores individuales, sobre los valores sociales o colectivos[124]. Constituye el Estado Social y Democrático de Derecho, y se aborda desde

---

[118] Comentarios y texto disponible en: http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/ConstEsp1812_1978/Const1837

[119] Texto disponible en: http://www.congreso.es/constitucion/ficheros/historicas/cons_1869.pdf

[120] Comentarios y texto disponible en: http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/ConstEsp1812_1978/Const1845

[121] Comentarios y texto disponible en: http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/ConstEsp1812_1978/Const1876

[122] Biblioteca Virtual de Miguel de Cervantes. Disponible en: http://www.cervantesvirtual.com/obra-visor/fuero-de-los-espanoles-de-1945--0/pdf/

[123] VARELA SUANZES - CARPEGNA, J. *Constituciones y Leyes Fundamentales*. Tomo I. Ed. Iustel. Madrid, 2012. pp. 117 y ss.

[124] CASAS BAAMONDE, Mª E., y RODRÍGUEZ – PIÑERO Y BRAVO – FERRER, M. (Directores). *Comentarios a la Constitución Española*. Título Primero. XXX Aniversario. Fundación Wolters Kluwer. Madrid, 2009.

una perspectiva social el reconocimiento de un auténtico catálogo de derechos fundamentales, que han de realizarse en ese marco político, por ser la estructura más adecuada para el ejercicio efectivo y la realización de las garantías procedimentales que regula, ya que su defensa y protección, es la base fundamental de la organización del Estado con un poder constituyente democrático, y así se afirman indubitadamente como inviolables e inherentes a la dignidad de la persona.

En este sentido, en el artículo 10 CE se establece que:

> "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, son fundamento del orden político y de la paz social".

La dignidad de la persona es un valor moral y espiritual, que constituye un mínimo invulnerable que debe ser asegurado por el orden jurídico y político constitucional. Es una cualidad que "corresponde a todo ser humano con independencia de sus concretas características particulares, y a la que se contraponen frontal y radicalmente comportamientos prohibidos en el artículo 15 CE, bien porque cosifican al individuo, rebajándolo a un nivel material o animal, bien porque lo mediatizan o instrumentalizan, olvidándose de que toda persona es un fin en si mismo"[125]. Es "un valor fundamental (...) reconocido en el artículo 10 como germen o núcleo de unos derechos que le son inherentes[126] es decir, un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consiguió la pretensión al respeto por parte de los demás"[127].

En un contexto democrático, en que la Constitución es instrumento de defensa de la dignidad humana, España confirma internacionalmente su compromiso con los derechos fundamentales adhiriéndose, con fecha 26 de

[125] STC 181/2004, de 2 de Noviembre. F.Jº. 13º.
[126] STC 53/1985, de 11 de Abril. F.Jº. 3º.
[127] Ibídem. F.Jº. 8º.

Septiembre de 1979, a la Convención Europea de Salvaguardia de los Derechos Humanos y de las Libertades Fundamentales (firmado en Roma el 4 de Noviembre de 1950)[128], que reconocía en su artículo 14: "El goce de los derechos y de las libertades fundamentales ha de ser asegurado a todos, sin distinción alguna". Y, adhiriéndose igualmente, en 1985 al Pacto Internacional de Derechos Civiles y Políticos de la ONU (firmado en Nueva York el 16 de Diciembre 1966)[129].

Pero sucede que los derechos fundamentales no implican sin más una absoluta preeminencia, sino que, bajo determinadas circunstancias podrán ser obligados a ceder en favor de otros intereses superiores.

La Constitución Española prevé reglas de obligado respeto en le desarrollo y delimitación de los derechos fundamentales, y son, a grandes rasgos, los principios de "reserva de ley" (STC 83/1984, de 24 de Julio. F.Jº. 4º), de motivación (STC 54/1995, de 24 de Febrero. F.Jº. 7º), de necesidad (STC 61/1982, de 23 de Octubre. F.Jº. 5º), de proporcionalidad (STC 37/1989, de 11 de Febrero. F.Jº. 7º) y de "contenido esencial" (STC 11/1981, de 8 de Abril. F.Jº. 10º) respecto de los derechos en conflicto.

Los derechos fundamentales tienen al individuo por sujeto activo y al Estado por sujeto pasivo, pues éste debe facilitarles a aquellos su ejercicio, procurándoles las condiciones más adecuadas, tendentes a evitar vulneraciones que los puedan hacer inexistentes. Regular condiciones que limiten el ejercicio de los derechos individuales, sólo será legítimo si es para alcanzar otros bienes o valores constitucionales.

---

[128] Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. Disponible en: http://www.boe.es/diario_boe/txt.php?id=BOE-A-1979-24010

[129] Instrumento de adhesión de 17 de enero de 1985, de España al Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos, adoptado en Nueva York por la Asamblea General de las Naciones Unidas, el 19 de Biciembre de 1966. Disponible en: http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1985-5259

En un Estado de Derecho todo individuo puede ejercitar su libertad, ya sea en conjunto con la sociedad, como en su esfera individual[130], y es en este segundo espacio, como una manifestación del derecho a la dignidad y al desarrollo libre de la personalidad, de la libertad de decisión y elección respecto de lo que cada individuo quiera para sí, dónde obra cobra sentido el precepto que centra la exposición, el artículo 18 CE. Este precepto representa para el legislador (y para la Administración Pública en general), un fortín de actividad marcado por la necesidad de garantizar la protección de un ámbito individual y familiar inexpugnable, como es el que se desarrolla dentro el domicilio, y en este sentido, partiendo de la idea de la esfera íntima y privada que éste guarda, se ha protegido a través del artículo 18 CE:

> "1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
>
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
>
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
>
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

La aparición de instrumentos mecánicos de colección de datos en el S.XX, que contribuían a realizar perfiles individualizados de los ciudadanos, puso el acento en las posibilidades técnicas de un gobierno de conocer aspectos detallados su personalidad, pudiendo controlar sus movimientos y, en consecuencia, tomar decisiones sobre su vida. Por este motivo, la

[130] Artículo 17 CE*:* "Toda persona tiene derecho a la libertad y a la seguridad. Nadie puede ser privado de su libertad, sino con la observancia de lo establecido en este artículo y en los casos y en la forma previstos en la ley".

Constitución de 1978 ya recogía expresamente el término "informática", y limitaba su utilización para preservar el "pleno ejercicio" de los derechos reconocidos en la misma, especialmente el honor y la intimidad personal y familiar.

Para su desarrollo y aplicación efectiva, se promulgó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD. Vigente hasta el 14 de enero de 2000).

Hasta ese momento, la protección de datos personales en España era una mera sombra sin delimitar, que se intuía bajo el mandato del artículo 18 de la CE, pero que tan sólo contaba con Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen. Esta norma, ya mencionaba en su Disposición Transitoria Primera que "en tanto no se promulgue la normativa prevista en el artículo dieciocho, apartado cuatro, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley". Esta disposición fue derogada en consecuencia por la Disposición Derogatoria Única de la LORTAD.

Con la LORTAD, se proporcionó a la protección de la información personal frente a la amenaza que estaba empezando a suponer el desarrollo tecnológico, un contenido preciso, y así, en el primer párrafo de su Exposición de Motivos explica que: "La Constitución española, en su artículo 18.4, emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La aún reciente aprobación de nuestra Constitución y, por tanto, su moderno carácter, le permitió expresamente la articulación de garantías contra la posible utilización torticera de ese fenómeno de la contemporaneidad que es la informática". Reconoce además la distinción entre la restrictiva "intimidad" y la más amplia "privacidad": "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". Y establece la necesidad del desarrollo precisamente porque: "las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos".

Para que derechos y privilegios puedan alcanzar la condición de "efectivos", primero han de estar formalmente proclamados en la constitución y ésta, ser tomada como referencia en el sentido de listado de derechos, ya sea escrita o no[131]. Además los poderes públicos en su actuación están vinculados indisolublemente a las libertades y derechos fundamentales de sus administrados, de manera que, además de existir previsiones legales del derecho, habrán de contemplarse previsiones legales precisas para que éstos puedan llevar a cabo su ejercicio frente a otros particulares, velen también para que puedan oponer sus derechos con las debidas garantías, directamente frente al Estado, de manera que conjuntamente con este presupuesto, los cauces jurídicos y procesales que velen por su razón de ser en el Estado de Derecho deben también ser estipulados formalmente, y de ello se debe encargar, por la lógica separación de poderes de todo Estado de Derecho (además de la propia Constitución), el poder legislativo a través de Leyes Orgánicas, Leyes Ordinarias y Reglamentos de desarrollo.

El desarrollo práctico de sus disposiciones vino de la mano del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (vigente hasta el 19 de abril de 2008), que ante su tardanza en aparecer, se "excusaba" en el propio texto de la aprobación

[131] (...) "la necesidad de articular unos mecanismos de tutela adecuados a los riesgos que, por este flanco de la información personal automatizada, amenazan a los individuos, explican que el legislador, explicitando el espíritu constitucional, se haya preocupado por fijar reglas objetivas sobre el tratamiento de estos datos, haya previsto procedimientos específicos de garantía para sus titulares" (...) LUCAS MURILLO DE LA CUEVA, P. "La construcción del derecho a la autodeterminación informativa". Jornadas sobre Tecnologías de la Información para la modernización de las Administraciones Públicas (TECNIMAP). Organizadas por el Ministerio de Administraciones Públicas en Salamanca en 1998. Disponible en http://www.csi.map.es/csi/tecnimap/tecnimap1998/sp14.htm#5

diciendo: "la falta de desarrollo reglamentario ha impedido disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consecuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica"[132]. Asimismo, la intervención directa de los poderes públicos vendría dada por el Real Decreto 428/1993, de 26 de marzo, por el que se aprobó el Estatuto de la Agencia Española de Protección de Datos, y que establecía regulación de la estructura orgánica de la Agencia de Protección de Datos, como ente independiente que debe garantizar el cumplimiento de las previsiones y mandatos establecidos en la ley.[133]

Tanto la LORTAD como su Reglamento de desarrollo, han sido luego actualizados, la primera por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[134] y, el segundo, por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13-12-1999, de protección de datos de carácter personal[135].

Pero para comprender el actual sistema legislativo en materia de protección de datos, además, hay que considerar la influyente tradición normativa y doctrinal internacional, de la que en parte ya se ha hablado.

Como primera formulación jurídica del concepto de derecho a la protección de datos personales en el mundo, del llamado "derecho a ser dejado solo" o en paz ("the right to be let alone", Juez COOLEY) o, el derecho a no ser perturbado ("my home is my castle" anglosajón), se presentó por primera vez en un trabajo publicado en 1890 por Samuel WARREN y Louis BRANDEIS[136], en el que debatían el contenido esencial de la "privacy" y, reivindicaban que el "common law" debía garantizar a las personas su derecho a decidir hasta dónde podían ser intervenidos sus sentimientos y emociones, en la más pura esfera de la intimidad (el derecho a no ser

[132] BOE núm. 151. 25 junio 1999. p. 24241.
[133] BOE núm. 106. 4 mayo 1993. p. 13244.
[134] BOE núm. 298. 14 diciembre 1999. p. 43088.
[135] BOE núm. 17. 19 enero 2008. p. 4103.
[136] WARREN SAMUEL D. y BRANDEIS LOUIS. "The right to privacy". *Harvard Law Review*, Vol. IV, nº 5, 15 – XII –1890, p. 193 y ss. Traducción al español de Benigno Pendas… Op. Cit.

molestado). En este primer momento, era un derecho enfocado hacia la consideración de la inviolabilidad de la persona como un derecho más de la personalidad, relacionado directamente con la dignidad de la persona. La intimidad era básicamente el derecho a elegir la soledad.

Como también se ha comentado WESTIN[137], ayudó a precisar la definición legal del concepto "self determination", entendiendo la "privacy" como el poder de controlar la información personal (autodeterminación informativa). Un derecho del individuo a decidir cómo y cuándo es comunicada a otros su información personal, es inherente a todo proceso de adaptación personal, pues constantemente cada sujeto va a ir ponderando la necesidad de privacidad, dependiendo del contexto social y de su necesidad de interactuar en la comunidad. La soledad, el aislamiento, la reserva e intimidad, o el anonimato, se considera que son diferentes formas en que se puede manifestar esa capacidad decisoria individual y privada, como elemento absolutamente necesario del sistema organizativo de cualquier sociedad que quiera sentirse libre. PROOSER sin embargo, fue muy crítico con esta forma de ver el contenido de la privacidad, distinguiendo hasta cuatro formas de dañarla ("privacy torts"[138]). Según este autor, el ataque a la privacidad se puede producir por la intrusión en asuntos privados del afectado, por revelar información privada referente al mismo, por la posibilidad de ofrecer al público una falsa imagen del afectado y, por la apropiación de información de él, y esto contribuyó a clarificar doctrinalmente el alcance de la privacidad, siendo así interpretado y aplicado por los tribunales americanos[139].

En territorio europeo, esta herencia sirvió de base para dotar de significado al específico derecho a la protección de datos personales, superándose la concepción negativa del derecho a la intimidad, como el derecho a excluir a terceros de la esfera privada de los individuos. El derecho a la protección de datos para los europeos es el derecho a decidir y controlar la información que identifica a un individuo en sociedad.

---

[137] WESTIN, A.F. Privacy and Freedom…. Op. Cit.

[138] PROSSER, W.L. "Privacy". *California Law Review*. nº 48. 1960. pp. 383 – 423. Disponible en: http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf

[139] PIÑAR MAÑAS, J.L. ¿Existe la privacidad?... Op. Cit. p. 23

El proceso normativo de regulación de la protección de datos, tiene su punto de partida en la década de los 60 y evoluciona lentamente en Europa hasta la década de los 90, momento a partir del cual ya podremos hablar del comienzo de su consolidación como materia autónoma e independiente, y de un reflejo normativo especializado en la garantía de la protección de datos en toda Europa.

En 1967 en el Consejo de Europa se constituyó una comisión consultiva de estudio de la potencial lesividad de la informática en relación con los derechos de las personas, especialmente, en su vida privada. Las conclusiones de sus trabajos se publicaron como la Resolución 509 de la Asamblea del Consejo de Europa, sobre los derechos humanos y nuevos logros científicos y técnicos.

La preocupación por la creación de bancos de datos en el sector privado, y también en el sector público[140], y las recomendaciones del Parlamento Europeo a los Estados miembros, para toma de precauciones contra todo abuso o mal empleo de la información[141], llevaron a Alemania (1977), Francia (1978), Austria (1978) y Luxemburgo (1979), a promulgar las primeras leyes nacionales en materia de protección de datos en Europa.

El Convenio 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, plasmó en su artículo 1 la diferencia entre dos derechos estrechamente relacionados: la vida privada y la protección de los datos de carácter personal[142], y las Declaraciones de Derechos Humanos[143], y

[140] El Comité de Ministros del Consejo de Europa recomendó a los Gobiernos de sus Estados Miembros, en la resolución 73(22) de 26 de septiembre de 1973, tomar medidas tendentes a la protección de la vida privada de las personas físicas frente al mal uso o abuso de los bancos de datos electrónicos en el sector privado, y en la resolución 74(29) de 20 de septiembre de 1974, frente al mal uso o abuso de los bancos de datos electrónicos en el sector público.

[141] Resolución del Parlamento Europeo, de 8 de mayo de 1979, sobre la tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática. Directrices de 23 de septiembre de 1980, relativas a la protección de la intimidad (privacy) y de la circulación transfronteriza de datos personales, adoptadas por el Consejo de la OCDE.

[142] Artículo 1. "El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")". Convenio 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas.

[143] La Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948 (artículo 12); la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica), de 1966 (artículo 11);

los acuerdos comunitarios como el de Schengen, apremiaban a los gobiernos de los Estados miembros, para que diesen luz sobre esta materia.

Desde el año 1990, la normativa europea se ha fortalecido, y ha ido consolidando su independencia de aquella inicial herencia doctrinal americana, aunque a pesar de ello, y del tiempo transcurrido desde que se empezara a entender la necesidad de la protección de los datos de carácter personal, aún existen muchas dudas prácticas sobre el alcance del derecho, y las medidas necesarias para lograr su respeto y garantía.

2.2.- El artículo 18.4 en la CE.

España vivió a finales de los sesenta y principios de los setenta las primeras manifestaciones de nuevas formas de amenaza sobre los derechos fundamentales respecto del uso de la informática y, especialmente, de su repercusión sobre el derecho a la intimidad. Se buscaban nuevas fórmulas para su protección jurídica y así, en 1970 se creó una Comisión Interministerial de Informática y, en 1976 se constituyó un grupo de trabajo en el seno de las actividades de la entonces Escuela Nacional de Administración Pública, que llegó a redactar un borrador de "Anteproyecto de Ley Reguladora del acceso a la información y de los bancos de datos" y se empezó a elaborar el Plan Informático Nacional.

Sorprende conocer cómo, en aquellos momentos, ya había en España una importante preocupación por lo que la informática podía llegar a suponer para la vida de las personas, incluso, que podía perjudicar en igual grado que beneficiar al desarrollo de sus derechos y libertades. Mientras que en otros países ya se estaba tratando este problema, en el nuestro, aún se veía sólo

---

el Pacto Internacional de Derechos Civiles y Políticos, de 19 de diciembre de 1966 (artículo 17); el Convenio Europeo de Derechos Humanos, de 4 de noviembre de 1959 (artículo8); las Directrices para la regulación de los archivos de datos personales informatizados, adoptadas mediante resolución 45/95 de la Asamblea General de Naciones Unidas; y, la Tratado de Niza de 7 de Diciembre de 2000, conteniendo la Carta de los Derechos Fundamentales de la Unión Europea (artículo8), publicada en el DOCE nº 364-1, el 18 de diciembre de 2000.

como un riesgo de la evolución de la sociedad y de las necesidades de protección de los individuos que la conforman.

Las posibilidades de almacenamiento y tratamiento de información personal de los ciudadanos que comenzaba a ofrecer la informática, se hacía más tentadora para los poderes públicos, quienes veían una capacidad de control ilimitada sobre sus administrados. La interrelación de informaciones personales permite la obtención de perfiles personales, pudiendo tomarse decisiones sobre los afectados, sin que sean consultados o sin que siquiera lo sepan[144]. La fiscalización económica y política de un individuo podía llevarse a cabo libremente, sin saber éste que cada dato que proporcionaban en un momento dado, para la correcta prestación de un servicio público, iba a ser continuamente puesto en relación con otros que ya obrasen en poder de la administración, elaborándose auténticos perfiles de comportamiento y personalidad de cada ciudadano y, todo ello supuestamente, lo sería con base en algún "interés general".

Como decía DANZIN, "es posible establecer mecanismos de control para detener los abusos del poder"[145], y en este sentido, la Constitución Española configuró en 1978 el artículo 18.4 de la CE, pero ¿cuáles fueron los pensamientos del constituyente hasta llegar a la conclusión de que era importante recoger su expresa mención?

PEREZ LUÑO consideró que era necesario preocuparse tanto de la defensa de las libertades individuales como del "control democrático y el ejercicio social de la tecnología informática"[146] y éste fue sin duda el fin último de la introducción del artículo 18.4 en la Constitución Española, aún partiendo de un análisis puramente individualista y directamente vinculado con la dignidad del ser humano.

---

[144] HEREDERO HIGUERAS, M.: "La informática y el uso de la información personal". *Ribero y Santodomingo: Introducción a la informática jurídica*. Ed. Fundesco. Madrid, 1986. p. 35.

[145] DANZIN, A. "Informática ¿técnica de opresión o de liberación?", *Nuestro Tiempo*, nº 262, Servicio de publicaciones de la Universidad de Navarra. 1976. p. 52.

[146] PEREZ LUÑO, A. E. "La protección de la intimidad frente a la informática en la Constitución española de 1978" *Revista de estudios políticos*. Nº 9. 1979. p. 69.

Los trabajos preparatorios de la Constitución acusaron la influencia de su antecedente portugués y, ya en el primer borrador, figuraba el artículo 18.4 dedicado a la informática: "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos", y así fue publicado en el Boletín Oficial de las Cortes nº 44 del 5 de Enero de 1978, integrado en el Título II "de los derechos y deberes fundamentales". Esta primera redacción fue finalmente modificada por un inciso que, en realidad, supuso el elemento clave para llegar a determinar su núcleo esencial y, que fue precisamente clave en el debate constitucional sobre este precepto. Las posturas mantenidas durante el debate[147], conviene exponerlas de manera sucinta, pero precisa, para mostrar el pensamiento de aquel momento, en el que se evidenció la existencia de dos tendencias maestras en las discrepancias doctrinales en torno al bien jurídico protegido por el artículo 18.4 de la Constitución. Debe señalarse, en primer lugar, que el diputado SANCHO ROF, integrado en el grupo parlamentario de la U.C.D., propuso la supresión de este precepto aludiendo, por una parte, a que el primer número del artículo tutelaba suficientemente los supuestos principales[148] y, por otra, al peligro que suponía para la perdurabilidad de la Constitución, mencionar expresamente la informática y obviar otros medios que ya existieran en la época o que pudieran aparecer en el futuro: "ha de limitar no sólo el uso de la informática, sino cualquier otro medio que viole ese derecho al honor y a la intimidad"[149], postura que compartía GASTÓN SANZ[150], del Grupo Parlamentario Mixto, y para la que solicitaba la inclusión de la expresión "uso de la informática y cualesquiera otros procedimientos que pudieran dañar el honor a la intimidad personal y familiar de los ciudadanos". Otras enmiendas en esta línea, fueron las expuestas por CARRO MARTÍNEZ y JARABO PAYÁ[151], de Alianza Popular, que solicitaban la supresión de este apartado, o bien la "sustitución de la palabra "informática" por la más sencilla y clara de "información". Destacar de entre las posturas expuestas en esta línea, la enmienda nº 339 del Grupo Socialista del Congreso, que pedía la exclusión del término "ciudadano" porque este derecho debía "referirse a todos los

[147] SAINZ MORENO, F. (Ed). *Constitución Española; Serie I. Trabajos Parlamentarios*. Cortes Generales. Servicio de Estudios y Publicaciones. Madrid, 1980. pp. 2581 – 2533. (En adelante, C.E.T.P.)
[148] Enmienda nº 716 al Anteproyecto.
[149] Enmienda nº 779 al Anteproyecto.
[150] Enmienda nº 79 al Anteproyecto.
[151] Enmiendas nº 2 y 16 respectivamente, al Anteproyecto.

hombres" y no sólo a aquellos que gozaran del status de o la condición política de "ciudadano", pues se trataba en todo caso de dar texto a la garantía de un derecho humano.

Los planteamientos que se manifestaron de acuerdo con incluir este apartado para la Constitución, lo hicieron en la sesión celebrada en el Congreso el 19 de Mayo de 1978[152], comenzando con la intervención de ROCA JUNYENT (Minoría Catalana), que remarcó señalando que si la propuesta quedaba limitada a la tutela del honor y de la intimidad, no se protegería el ejercicio de otros derechos como el de asociación, de reunión, de gestión o iniciativa económica, etc., insistiendo en que su enmienda (la nº 117) "fundamentalmente supone el incorporar entre los límites de la informática el de que se garantice el pleno ejercicio de los derechos por parte de los ciudadanos. Mantiene para defenderlo que es evidente que la informática está planteando problemas graves en los países más desarrollados de interferencias e injerencias en la libertad del ciudadano".

MARTÍN TOVAL por su parte, y por el Grupo Socialista de Cataluña, sostuvo que "El tema es muy importante. Parece que estamos hablando de una técnica más, pero es una técnica cada vez con más incidencia en el ámbito de estos derechos individuales a que nos estamos refiriendo. Es evidente que existe una tendencia objetiva hacia la autorización creciente de la informática, penetrando en el dominio de lo que debe ser estrictamente la privacidad de la independencia y de la libertad del ciudadano. Consideramos por tanto muy útil que en la Constitución se hable sobre este tema y justamente en este precepto. Asimismo que se establezca una cláusula de garantías de protección de esos derechos; que se incluya ya en el texto de la Ponencia, pero también con referencia específica a la plenitud del ejercicio de todos los demás derechos reconocidos a la persona en la Constitución" y completa la exposición diciendo que "la informática es una técnica que proporciona una capacidad de control creciente sobre las vidas y circunstancias de los individuos y, por el contrario (...) es muy difícil que una auténtica capacidad de control sobre esa creciente capacidad de control que

[152] C.E.T.P. Tomo I. p. 1069. (*Diario de Sesiones del Senado-Comisión de Constitución*, 19 de Mayo de 1978, nº 70, p. 2527).

es el uso de la informática en manos del ejecutivo"[153]. Se pretendía una Constitución que perdurase con el paso del tiempo y, en general, estas motivaciones que compartieron JIMÉNEZ BLANCO (senador por UCD) y ZARAZAGA BURILLO (senador en el Grupo Mixto), defendían estos argumentos aludiendo a que "el actual estado de tecnología y los, sin duda, seguros avances que en ésta se van a producir, originarán el empleo de otros medios que deben ser sometidos al mismo tipo de limitaciones que el de la informática"[154]. Se subrayaba la importante necesidad de ampliar la referencia a la informática a otros procesos tecnológicos que pudieran afectar al pleno ejercicio de los derechos y libertades.

Finalmente, cuando se logró elaborar un proyecto de Constitución por la Comisión Mixta Congreso-Senado (publicado el 28 de octubre de 1978 en el Boletín Oficial de las Cortes), fue remitido a las Cámaras para ser aprobado por separado en cada una de ellas. El Pleno del Congreso de los Diputados lo aprobó por 316 votos a favor, 6 en contra y 3 abstenciones, y el Pleno del Senado, lo aprobó por 226 votos a favor, 5 en contra y 8 abstenciones. Es interesante reflejar estas votaciones, porque nos muestran el mayoritario interés que había entre aquellos representantes para dotar al pueblo de un completo catálogo de derechos y libertades. Esto nos da además una indicación de cómo las circunstancias del momento histórico, en que se someten a aprobación normas de este calibre, influyen decisivamente en el resultado. El 1978, tras la dictadura, el clamor era por la libertad y por la posibilidad real de ejercitar los derechos individuales y así, en el referéndum convocado el 6 de diciembre de 1978 para aprobar la Carta Magna, de casi 18 millones de votantes españoles, 15 lo hicieron a favor. Sin embargo, casi 30 años después y, en un contexto que supera las fronteras estatales, hemos visto cómo el proceso para la Constitución Europea, se ha visto paralizado (aún con la esperanza de muchos de no darlo por muerto) por la negativa de los ciudadanos europeos, consultados en sus países, a dotarse de esa norma suprema. Todo ello no es sino fruto de las circunstancias históricas del momento.

[153] C.E.T.P. Tomo I. p. 1070. (*Diario de Sesiones del Senado-Comisión de Constitución*, 19 de Mayo de 1978, nº 70, p. 2528).
[154] C.E.T.P. Tomo III. p. 3254. (*Diario de Sesiones del Senado-Comisión de Constitución*, 24 de agosto de 1978, nº 43, p. 1848).

La previsión constitucional de un derecho fundamental, exige si duda reconocer la necesidad de dotarlo además de un contenido aplicable a la práctica, que detalle las circunstancias y posibilidades de defensa de sus destinatarios, a fin de impedir que se convierta en un mero "derecho de papel". Su interpretación constitucional es necesaria "cuando debe darse contestación a una pregunta de Derecho Constitucional que, a la luz de la Constitución, no ofrece una solución clara". Cuando el Texto Fundamental se aplica por primera vez a un nuevo presupuesto de hecho, lo que en realidad se produce es una actualización de la norma fundamental"[155].

El constitucionalismo nace sobre la tradición europea que desconfía del Estado, como posible fuente de transgresión de los derechos del hombre, y por ello intenta limitarlo. La Constitución es norma superior y expresión de la soberanía del pueblo, y así, toda actividad del Estado, todas las leyes y, cualquier interpretación que de éstas se haga por los tribunales, se ha de subordinar a ella, y el Tribunal Constitucional será el órgano competente para resolver sobre cuantas cuestiones se planteen en este sentido.

Dotar de contenido a los conceptos jurídicos y a los principios constitucionales, no es un simple fenómeno de aplicación de la norma, debe tenerse en cuenta también el entendimiento de los ciudadanos, pues es el que va a determinar la vivencia real de la norma, explicando su actualización y en definitiva la cultura que debe atender. "La Constitución va suponiendo cada vez más un conjunto de normas subconstitucionales que pueden hacer llegar a olvidar después de X tiempo el significado primitivo del texto, produciendo el fenómeno de la "concretización" y "actualización al crearse subnormas que se imponen a todo acto, normativo o no, de rango inferior"[156].

[155] ALONSO GARCÍA, E. *La interpretación de la Constitución*. Centro de Estudios Constitucionales. Madrid, 1984. p.1. El autor cita a Hesse [*Grundzüge des Verfassungsrecht der Bundesrepublik Deutschland*, 11 ed., 1978, pp.20 - 21], explicando el proceso de subsunción, es decir, el proceso de creación de nuevas normas que delimitan y especifican el contenido de las genéricas (las constitucionales), que a primera vista son las únicas aplicadas. Esta norma "subconstitucional" surge de la parte dispositiva de las Sentencias, formulada en términos abstractos , de modo semejante a una norma jurídica.
[156] Ibdem. p. 12.

Sin entrar en el debate de si la interpretación del Tribunal Constitucional, es o debe ser jurídica o política[157], pues se considera que ambas son necesarias y solo útiles como una única, se puede afirmar que la jurisdicción constitucional en nuestro país es el mecanismo que por excelencia va a sustentar la flexibilidad y capacidad de adaptación del sistema jurídico a la realidad que ordena. Toda interpretación que se haga de la Norma, ha de resultar siempre en un presupuesto lógico y coherente que las dote de significado. Debe tenerse en cuenta no sólo su entorno normativo sino también social, político, económico, etc., porque todas las normas que contiene la Constitución son piezas en el Estado de Derecho y, entenderlas en uno u otro sentido, en uno u otro momento, es lo que va a delimitar la interrelación de los poderes públicos y los individuos, precisamente ahí radica la importancia que debe darse a las decisiones del Tribunal Constitucional. Independientemente de que se utilice un criterio interpretativo material, formal, sistemático o evolutivo, la ponderación interpretativa del jurista es la que debe aportar a sus destinatarios la seguridad de que, aun siendo "gobernados" por normas que fueron dictadas en un momento en que las necesidades existentes las requerían así, tenían un sentido concreto, no han cambiado en su esencia, sino en el sentido en que eran interpretadas entonces.

El cometido del conjunto de las normas constitucionales debe ser el de marcar fronteras para el intérprete, que no podrá traspasar si quiere respetar el sistema establecido. Siguiendo a PÉREZ LUÑO[158], los principios interpretativos básicos que deben guiar al Tribunal Constitucional en su tarea son:

> a) Principio de la "unidad" constitucional: el conjunto de normas constitucionales forman una totalidad coherente, y es necesario dotarlas de un sentido integrador.

[157] "Una Constitución sin un Tribunal Constitucional que imponga su interpretación y la efectividad de la misma en los casos cuestionados en una Constitución herida de muerte, que loga su suerte a la del partido en el poder, que impone en esos casos, por simple prevalencia fáctica, la interpretación que en ese momento le conviene". GARCÍA DE ENTERRÍA, E. *La Constitución como norma y el Tribunal Constitucional.* Ed. Civitas. Madrid, 1985. pp. 199 y ss. Y, *Curso de derecho administrativo*. Vol. I. Ed. Civitas. Madrid, 2008.

[158] PÉREZ LUÑO, A. *Derechos Humanos, Estado de Derecho y Constitución*. Ed. Tecnos. Madrid, 1984. p. 277.

b) Principio de la "funcionalidad": el marco en que se protegen las normas se compone de poderes con funciones concretas asignadas, y así deben ser respetadas.

c) Principio de "eficacia o efectividad": la aplicación práctica de lo interpretado debe responder a criterios de máxima eficacia que en ningún caso distorsione su contenido esencial.

Sin embargo, KONRAD HESSE contempla la labor interpretativa, como un esfuerzo determinante para concretar las lagunas a interpretación constitucional, buscando no tanto comprender como concretar los preceptos, y para ello deben dejarse de lado los métodos clásicos de interpretación. Según este autor, los principios interpretativos que ha de seguirse son[159]:

a) El principio de "unidad" de la Constitución: La interpretación de la Constitución debe considerarla un conjunto armónico y sistemático, a partir del cual se va a organizar el sistema jurídico.

b) El principio de "concordancia práctica": Todo conflicto entre disposiciones constitucionales debe solucionarse sin sacrificios, es decir, ponderando de forma equilibrada los valores, derechos o principios afectados, y considerando que todo precepto constitucional está orientado a la protección de los derechos fundamentales, y éstos, considerados como manifestaciones de la dignidad humana, cuya defensa es el objetivo principal del Estado.

c) El principio de "corrección funcional": El juez constitucional debe respetar en todo caso las competencias de los órganos constitucionales, al realizar su labor

[159] HESSE, K. *Escritos de Derecho Constitucional*. Traducción de Pedro Cruz Villalón. 2ª Ed. Centro de Estudios Constitucionales. Madrid, 1992. pp. 45-47.

interpretativa, de forma que así se garantice plenamente el respeto de los derechos fundamentales y, con ello, el equilibrio propio del Estado Constitucional.

d) El principio de "función integradora": El resultado de la interpretación constitucional deberá contribuir a ordenar y armonizar las relaciones de los poderes públicos entre sí, y las de éstos con los ciudadanos.

e) El principio de "fuerza normativa": La interpretación debe dirigirse a fomentar el respeto de la Constitución como norma jurídica, vinculante para todo poder público y para la sociedad.

Por otra parte, para HESSE, el sentido de la interpretación es el de encontrar el resultado constitucionalmente correcto a través de un procedimiento racional y controlable, creando certeza, previsibilidad y seguridad jurídica. En este sentido, considera que "la Constitución debe permanecer incompleta e inacabada por ser la vida que pretende normar vida histórica, y en tanto que tal, sometida a cambios históricos". Su fuerza normativa radica en su pretensión de vigencia, de adaptación a las circunstancias, así "la primacía de la Constitución escrita no la convierte en la última fuente del derecho", es más, "la Constitución debe su legitimidad al acuerdo en torno a su contenido o al menos al respeto del mismo. Pero ni siquiera el más completo acuerdo es capaz de excluir una contradicción entre la constitución y los más altos principios del Derecho como último fundamento de la legitimidad. Cuya fuerza de obligar, sin embargo, no puede ser constatada por ninguna otra instancia sino por la conciencia jurídica"[160].

Si bien la Constitución es el orden jurídico supremo de la comunidad, no puede entenderse que lo regula todo, sino sólo los aspectos más importantes o especiales de la vida social y estatal, dejando el resto a la configuración particularmente del legislador[161].

[160] Ibídem. pp. 19, 22 y 23.
[161] HESSE, K. *Derecho Constitucional y Derecho Privado*. Ed. Civitas. Madrid, 1995. p. 83.

Centrándonos en la tarea interpretativa del Tribunal Constitucional, es preciso señalar que no siempre ha mostrado la rigidez[162] que se le presupone, si no que el problema se ha manifestado cuando los posicionamientos políticos y el puro sentido de la evolución, han originado sentencias a veces contradictorias. Sí es cierto que la tónica habitual en España es de gran respeto por los antecedentes interpretativos en materia constitucional pero, es inevitable que en función de las circunstancias que se den en el momento en que van a ser aplicados, se siga una u otra corriente, se delimite uno u otro alcance. Con todo ello, el Alto Tribunal tiene una ardua labor en la defensa y protección de la Constitución y, de todos aquellos que bajo su mandato conviven, pues su valor normativo no es otro que el de velar por la estabilidad del Estado donde se promulga y con esta intención debe ser interpretada.

La Constitución protege a las personas garantizando que sólo determinado poder y, de determinada forma, puede limitar la libertad. En este sentido, los derechos fundamentales (entendidos como algo vivo) necesitan especialmente adaptarse al progreso del ser humano y de la sociedad en que éste se desarrolla, evitando la rigidez propia de toda norma escrita. El ser humano exige como parte de la sociedad unas normas de convivencia que respeten la esencia de su naturaleza en el contexto histórico en que vive y, sólo si esto se cumple, sus derechos podrán ser dotados del significado práctico que exigen las circunstancias.

El intérprete debe conocer sus parámetros, su ámbito de aplicación y su validez, debe guiarse en todo caso por el hecho de que las principales tesis sobre la interpretación de los derechos fundamentales persiguen igual objetivo: delimitar el alcance de los derechos, bien de forma universal y

[162] Por ejemplo, el Tribunal Constitucional matiza su doctrina precedente para adaptarla a la evolución del proceso autonómico. Así, las SSTC 15/1989 y 103/1989 inician una nueva línea jurisprudencial en relación con la cláusula de supletoriedad del derecho estatal, de modo que se establece que dicha cláusula no puede ya identificarse con una cláusula universal que permita al Estado el ejercicio de competencias normativas sobre cualesquiera materia. Otro ejemplo de la evolución en los criterios jurisprudenciales es lo ocurrido con la resolución del TC de 26 de febrero de 1990, que inadmitió la demanda de amparo de Doña Gregoria López Ostra frente a las inmisiones originadas por los malos olores, el humo y el ruido de una planta depuradora de aguas residuales de la ciudad de Lorca (Murcia), que posteriormente vendría a ser enmendada por el TEDH en la sentencia de 9 de diciembre de 1994, criterio que, en la sentencia 119/2001 del TC, vino a fijar un alcance mucho más amplio, (que ya se esbozaba en la anterior STC 199/1996 de 3 de diciembre de 1996), con base en una interpretación del artículo 18 CE a la luz de la jurisprudencia gestada por el TEDH sobre el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

atemporal bien de forma concreta y en el momento en que deben ser atendidos sus destinatarios[163], y todo ello, teniendo en cuenta además que el sistema de positivación de los derechos fundamentales no siempre es el mismo, porque pueden ser insertados en la Norma bien como valores o principios generales (superiores) o bien, pueden ser planteados siguiendo un criterio casuístico (pormenorizando el alcance de cada uno de ellos). La cuestión es que cada valor o principio de la Constitución sea encajado en el entramado normativo de la forma más eficiente posible.

Tras la II Guerra Mundial el respeto a los programas de derechos fundamentales existentes, era exigido firmemente con compromisos, que pretendían serlo para todas las partes, que así los reconocían ratificándolos, y sobre lo que, al reestablecerse un sistema aparentemente estable de derechos, aparecieron los problemas para su interpretación. La tarea de determinar el verdadero significado y propiedades de la esencia del ser humano retomó entonces las teorías iusnaturalistas, positivistas, e intermedias. En el ámbito Europeo, los Estados iban entendiendo la importancia de una Constitución (no todos lo hicieron), se comenzaba a fraguar un espacio de libertades, de obligaciones y derechos de alcance superior al que pudiera tener la normativa meramente estatal.

La obligación establecida por el artículo 53.1 de la CE[164] hace que el alcance de las interpretaciones de los juristas no exceda en ningún caso del núcleo básico, por cuanto se desvirtuaría el contenido esencial de cualquier derecho. La Constitución, como garantía[165] de positivación y de interpretación, debe orientar a quien quiera acercarse a desentrañar la intención de un derecho fundamental y su verdadero significado dentro del Estado de Derecho, debe en definitiva, acercar a los destinatarios de sus previsiones a las condiciones para el ejercicio de los derechos. Surge entonces la duda sobre la capacidad innovadora del intérprete ¿es el Tribunal Constitucional un ente capaz de crear derechos?

---

[163] En el contexto de la presente investigación, este último será el alcance que trataremos de determinar, en concreto, para el artículo 18.4 de la CE.

[164] Artículo 53. 1. CE. Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos".

[165] RUBIO LLORENTE, F. *La Constitución como fuente del Derecho*. Col. La Constitución española y las fuentes del Derecho, Vol. I, Instituto de Estudios Fiscales. Madrid, 1979. p. 66 y ss.

Sin exponer los argumentos de las distintas corrientes doctrinales que resuelven a favor o en contra, veremos más adelante que uno de los ejemplos más claros que tiene la Constitución Española, el artículo 18.4 de la CE tiene elementos suficientes para desechar la idea del Alto Tribunal como ente "creador de derechos fundamentales"[166] al menos, en sentido estricto.

El jurista HANS KELSEN trata el tema de la Interpretación en el Capítulo X de su obra "Teoría Pura del Derecho" y señala que, la interpretación es una operación del espíritu que acompaña al proceso de creación del derecho al pasar de la norma superior a una inferior. Según KELSEN, se interpreta cuando el juez va a aplicar la ley referida al caso concreto y, también cuando el legislativo legisla, pero siempre dentro de los límites determinados por la Carta Magna, "toda norma es interpretada en la medida en que se desciende un grado en la jerarquía del orden jurídico para su aplicación". KELSEN acepta que la norma superior es un marco abierto a varias posibilidades y, que tanto la creación de la norma como la propia interpretación son actos de voluntad cuya emisión viene establecida en la Constitución: la voluntad creadora de normas debe emanar sólo del Parlamento en representación del pueblo y en su función legisladora, la voluntad interpretativa se abre a los tribunales para completar la primera ("función creadora indirecta" o mejor expresado, "función integradora").

Entendida pues la tarea de interpretación del Tribunal Constitucional, como una función eminentemente integradora debe ser puesta en un contexto jurídico (de la Teoría del Derecho) y, en un contexto político en evolución, en los que se esté produciendo dicha interpretación para el caso concreto. Aplicar el Derecho (conjunto de normas) conforme a las pautas que se han ido marcando por las propias necesidades de la sociedad, va a dar lugar a conclusiones que permiten acercar lo positivado (no siempre en sentido estricto, como se ha visto) a la realidad de los individuos a quienes se destina y viceversa. La realidad puede, o más bien debe servirse de este cauce para acercarse a las normas, puliéndolas y configurándolas para el orden social que quieren regir. Establecidos los dos puntos de vista, y viendo

[166] FERNÁNDEZ SEGADO, F. La obsolescencia de la bipolaridad "modelo americano – modelo europeo – Kelsiano" como criterio analítico del control de constitucionalidad y la búsqueda de una nueva tipología explicativa. *Parlamento y Constitución. Anuario de las Cortes Castilla la Mancha,* Nº 6. 2002. pp. 9 -74.

como ambos se nutren el uno del otro (normas ⇔ realidad), detengámonos en destacar la labor del mecanismo que lo hace posible en el Estado de Derecho: el poder judicial.

> "La función del juez entraña, fundamentalmente al menos un juicio lógico, consistente en la aplicación de una norma de una ley a un caso concreto. La tarea de juzgar implica tomar una decisión, que es la consecuencia lógica y necesaria de la constatación del Derecho objetivo, y consiguientemente, también de los derechos subjetivos. A diferencia de la Administración, que ha de preocuparse de modo preponderante del interés público, la jurisdicción está al servicio del Derecho y la justicia a través del conocimiento de los hechos y la aplicación de las normas"[167].

No es por tanto una tarea mecánica de aplicación de la norma a los hechos, sino que entraña todo un proceso racional y de conciencia sobre "hechos probados", interpretándolos para incardinarlos en la normativa. Nunca puede, ni debe, entenderse la interpretación judicial como el capricho del juez, y de ahí que el expuesto sea el camino lógico a seguir para dar curso a tales tareas (hecho → norma), y no al revés.

Además de la función interpretativa vista, debe tenerse en cuenta la "función creadora de la jurisprudencia". Es cierto que la legislación presenta a veces imprecisiones que dificultan su comprensión y su aplicación práctica, sin embargo, existe un principio informador del derecho que determina que el Derecho siempre tiene soluciones, aunque para ello deba recurrir a instrumentos subsidiarios.

El juez al sentenciar, debe completar las lagunas que presenta el ordenamiento jurídico y, de esta forma, realizar una función más que de creación, de integración del Derecho, porque la seguridad jurídica impide hablar de estricta "creación del derecho". El sentido común nos dice que,

[167] CASTÁN TOBEÑAS, J. *Poder Judicial e independencia judicial*, Ed. Reus. Madrid, 1951. p. 46.

ciertamente conectar una decisión de voluntad con la norma, para aplicarla al caso concreto, no es exactamente "crear" sino más bien, "adaptar".

En términos generales, en el ordenamiento español, "la jurisprudencia complementará el ordenamiento jurídico con la doctrina que, de modo reiterado, establezca el Tribunal Supremo al interpretar y aplicar la ley, la costumbre y los principios generales del Derecho"[168] pero, en materia concreta de derechos fundamentales, el Tribunal Constitucional es el órgano que dará sentido a su respeto.

La jurisprudencia que emana de sus decisiones es la que va a dar luz sobre el verdadero sentido de estos derechos de rango especial y lo va a hacer siempre en función del momento histórico, político y social que estén viviendo sus destinatarios. Esta preeminencia de las decisiones del Tribunal Constitucional, está marcada necesariamente por el organigrama institucional y político en un Estado de Derecho de corte constitucionalista. Para hacer realidad de manera efectiva el contenido de la Norma Suprema y, proteger en el sentido más estricto el ejercicio efectivo de los derechos humanos, su jurisprudencia interpreta la Constitución, la hace real.

2.3.- Legislación y contribución jurisprudencial.

El conjunto de normas que regulan en España el derecho a la protección de datos personales se ha ido elaborando en coherencia con el contenido de la normativa comunitaria, pero lógicamente, han contribuido a su delimitación tanto la jurisprudencia de aplicación originada en los Tribunales españoles como las decisiones de las diferentes Agencias de Protección de Datos del territorio. Todo ello ha jugado un importantísimo

[168] Artículo 1.1 Código Civil español.

papel en la determinación de los aspectos más prácticos y de las garantías de la protección de los datos personales en el territorio español.

La primera norma que desarrolló el contenido del derecho fundamental a la protección de datos, recogido en el artículo 18.4 de la CE, fue la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD). En la Exposición de Motivos señalaba ya que debía distinguirse entre las garantías constitucionales necesaria para la intimidad y para la privacidad: "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". Esta Ley se inspiró en la Ley Federal de 27 de enero de 1977, para la protección contra el abuso de datos sobre las personas con motivo del tratamiento electrónico de datos en la República Federal Alemana, pero el referente verdadero es el Convenio 108 del Consejo de Europa de 1981, coincidiendo en definiciones, principios básicos, categorías de datos, garantías complementarias, etc. Sin embargo, se puede hablar de diferencias[169], por ejemplo, que el Convenio (artículo 3. 1) expone que se aplicará a ficheros y tratamientos de carácter público y privado, automatizados, y la LORTAD, distinguía directrices para ambos sectores, para cuestiones como la cesión de los datos o para el régimen sancionador (arts. 11.2.e), 19 y 45) y, se aplicaba también a ficheros de carácter no automatizado, previo informe del Director de la Agencia.

El objeto específico de la aplicación de los preceptos de esta Ley era la "información personal": artículo 2, párrafo 1º "La presente ley será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado".

[169] MARTÍN-CASALLO LÒPEZ, J.J. "La Directiva 95/46/CE y su incidencia en el ordenamiento jurídico español". Jornadas sobre el derecho español de la protección de datos. Agencia de Protección de Datos. 28, 29 y 30 de Octubre de 1996, Madrid. p. 15.

Esta norma no se circunscribía únicamente a un ámbito privado o íntimo, ni lo hacía para referirse solamente a una esfera virtual[170], sino que ya se afirmaba la tesis de un derecho fundamental autónomo y preexistente, que debía ser protegido para preservar la libertad y la dignidad de los ciudadanos. Sin embargo, como se ha mostrado con la referencia jurisprudencial, no fue tarea sencilla darle forma[171].

Con la aparición de la LORTAD se "legalizaron" definiciones básicas como la de "dato de carácter personal", que lo es cualquier información concerniente a personas identificadas o identificables, y excluyendo lo relativo a las personas jurídicas; o la del "tratamiento de datos" que incluía tanto los tratamientos automatizados como los que no lo son. Por otra parte, por primera vez se estructuraron los principios ordenadores de la protección de datos: la "pertinencia de los datos" (artículo 4), como la calidad de los datos, exactitud y su posibilidad de rectificación, siendo exclusivamente utilizados para el fin para el que fueron recogidos[172]; la "información" (artículo 5), como el derecho a saber quién, cómo y cuándo se van a utilizar sus datos personales; el "consentimiento" (artículo 6), como la obligación de solicitar el consentimiento al afectado antes de proceder a recabar y/o utilizar sus datos; la "seguridad de los datos" (artículo 9) y, el "deber de secreto" (artículo 10), como las obligaciones de mantener el secreto

[170] (...) "el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado". En la exposición de motivos de la Ley 15/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

[171] "Tal es la importancia de este nuevo entorno que ya estamos viviendo que el Derecho no puede desconocerlo. La tradicional lentitud de las leyes a la hora de regular nuevas figuras y realidades sociales se hace aquí aún más dramática donde el fenómeno crece a ojos vista en cuestión de meses, incluso de días". SALGADO SEGUÍN, V.A. "Protección jurídica de los datos personales: Aproximación a la LORTAD", publicado en la página web de la Universidad de Alicante, en *Guías de Interés: Protección de Datos*. 1998. http://www.ua.es/oia/es/legisla/articulo.htm

[172] (...) "advierte que cualquier dato en principio neutro e irrelevante puede convertirse en sensible a tenor del uso que se haga de él26, de modo que estos abusos pueden llevarse a cabo con independencia tanto de la calidad del dato singular que pudiera ser descubierto, como de la capacidad genérica de los sistemas para operar con datos aparente o aisladamente inocuos, pero relevantes desde el punto de los derechos y libertades aludidos en cada caso, en tanto son susceptibles de tratamiento". PÉREZ LUÑO, A.E., "Comentario legislativo: la LORTAD y los derechos fundamentales", *Derecho y Libertades.Revista del Instituto Bartolomé de las Casas*, 1993. p. 413

profesional respecto de los datos, y el deber de guardarlos "evitando eviten su alteración, pérdida, tratamiento o acceso no autorizado"[173].

La LORTAD trataba de buscar un equilibrio sensato entre los principios adoptados doctrinalmente y el derecho de las personas a decidir sobre su información personal, a acceder, rectificar o cancelar su información personal en manos de terceros, pero nació con vicios de inconstitucionalidad que fueron inmediatamente puestos de manifiesto por el propio Defensor del Pueblo, junto con el Consejo Ejecutivo de la Generalidad de Cataluña, el Parlamento de Cataluña y el Grupo Parlamentario Popular, interponiendo el preceptivo recurso ante el Tribunal Constitucional. Se impugnaron, el artículo 6.2 (por considerar que dejaba vacío de contenido los límites que deben imponerse a la informática tal y como ordena taxativamente el apartado 4 del artículo 18 CE, al eximir a la administración de la obligación de recabar el consentimiento del afectado para proceder al tratamiento de sus datos personales y su cesión entre administraciones públicas); el artículo 19.1 (por infracción de la reserva de Ley dispuesta en el artículo 53.1 CE); los artículos 20.3 y 22.1 (por imponer graves excepciones a los derechos de los ciudadanos, respecto de los datos que obrasen en ficheros de las Administraciones Públicas, cuando su ejercicio impida o dificulte gravemente las funciones de control y verificación de las Administraciones Públicas o la persecución de infracciones también administrativas)[174], y también los artículos 24, 31, 39.1 y 2, 40.1 y 2, relativos a las funciones que la LORTAD atribuía a la Agencia de Protección de Datos y al Registro General, respecto de ficheros de titularidad privada ubicados en Cataluña.

Además, pronto se quedaría obsoleta, pues dos años después eran aprobadas las Directiva 95/46/CE, de 24 de octubre y la Directiva 97/66/CE, de 15 de diciembre, ambas del Parlamento Europeo y del Consejo, exigiendo una revisión del régimen jurídico vigente, y que finalmente se materializaría con la aprobación de la Ley Orgánica de Protección de Datos Personales

[173] PÉREZ LUÑO, A.E.: *"Sobre el arte legislativo de birbiloque. La LOPRODA y la tutela de la libertad informática en España", Anuario de Filosofía del Derecho*, de la Sociedad Española de Filosofía Jurídica y Política. 2001. p. 346. También, DEL PESO NAVARRO, E. y RAMOS GONZÁLEZ, M.A.: *LORTAD. Reglamento de Seguridad*, Díaz de Santos. Madrid, 1999. p. 130.
[174] ÁLVAREZ-CIENFUEGOS SUÁREZ, J.M. *La defensa de la intimidad de los ciudadanos y la tecnología informática*. Ed. Aranzadi Editorial. Navarra, 1999. p. 39.

15/1999 (LOPD). A la entrada en vigor de esta norma, aquellos recursos no habían sido aún resueltos, por lo que cuando llegó el momento, el Tribunal Constitucional sólo entró a conocer del fondo de aquellos preceptos que habían sido transcritos en la nueva norma, resultando de su análisis constitucional las ya famosas Sentencias 290/2000 y 292/2000[175].

La Directiva 95/46/CE fue incorporada al ordenamiento jurídico español cuatro años después, a través de la LOPD, pasando a establecer con mayor detalle los principios de la protección de datos, en armonía con el derecho comunitario. Por ejemplo, se estableció de forma expresa que las normas relativas a la protección de datos serían aplicables tanto a ficheros automatizados como a ficheros manuales. Además, se tuvo muy en cuenta la doctrina jurisprudencial de la STC 254/1993, de 20 de Julio, de forma que se reconoció que los ciudadanos tenían derecho a saber lo que las Administraciones Públicas conservaban de su información personal, y los tratamientos a que podían someterla, es decir, tenían derecho a conocer la existencia de los ficheros, los fines para que se creaban y utilizaban, y los responsables de dichos ficheros.

La LOPD de 1999, regula aún hoy todo el sistema de la protección de datos de carácter personal. Sin entrar en detallar sus preceptos podría decirse que, en general, a pesar de no tener exposición de motivos, su espíritu (su contenido) mantiene una clara desvinculación del ámbito de la intimidad y, que además, al citar un plazo concreto para ser de aplicación tanto a ficheros automatizados como a los no automatizados, demuestra la necesidad de entender el derecho a la protección de datos personales, con entidad propia e independiente del uso que se pueda hacer de la informática en perjuicio de los individuos.

La Disposición Adicional Primera de esa norma dice textualmente que, en "el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo

[175] *Jurisprudencia constitucional*, Vol. 58 Tribunal Constitucional, Boletín Oficial del Estado. 2002. pp. 1010 - 1025.

anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados", lo que significa que desde el año 2007, los tratamientos de datos de carácter personal que se hayan hecho conculcando alguno de los preceptos de esta Ley, utilizando o no la informática, eran susceptibles de ser denunciados y castigados. Esto sin duda ha sido el paso definitivo para el punto final de la tesis que se viene defendiendo en materia constitucional, junto con la aprobación de un nuevo Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, el día 21 de Diciembre de 2007.

La LOPD, debido al veloz desarrollo de la tecnología, no es un texto que se pueda considerar hoy acorde con las circunstancias de progreso de la Sociedad de la Información, ni siquiera con la jurisprudencia que en teoría la ha ido interpretando, o con algunas de las normas que se han ido dictando a nivel europeo. Se señalan por ejemplo, como aspectos más significativos de sus carencias, la inexistencia de una previsión específica sobre el tratamiento de datos personales de menores, la permisividad con que se regula el "Censo Promocional"[176], la exclusión de la materia de terrorismo de su aplicación, ignorando las previsiones estipuladas sobre ello en el Convenio Europol[177], la "incompatibilidad" del artículo 4 en relación con el tratamiento de datos

[176] "Esta figura, desconocida de la LORTAD, ha sido introducida por la LOPD, con el fin de regular y enmarcar el uso del Censo Electoral por las empresas de marketing. Este tratamiento, ya declarado ilegítimo por la LORTAD, aparecía de difícil control por la AEPD, considerando el elevado número de sanciones que fueron pronunciando a raíz de la LORTAD. El legislador introdujo esta figura con el fin de prevenir dichos abusos y de la misma forma zanjó la polémica desatada a raíz del artículo 39.3 de la Ley 7/1996, de 15 de enero de ordenación del comercio minorista, que establece que los datos de identidad y de domicilio contenidos en el censo electoral tienen el carácter de datos accesibles al público y por lo tanto son utilizables por las empresas de publicidad directa y venta a distancia, así regulado, tanto la AEPD como la Junta Electoral Central se pronunciaron en contra de tal interpretación, por el carácter ordinario y sectorial de dicha ley que en ningún caso la habilita para modificar leyes con carácter orgánico (...). Nos encontramos ante una situación que ya había sido denunciada en la Sentencia del Tribunal Constitucional alemán en el año 1983, del censo, y que puso la primera piedra del reconocimiento europeo, a nivel constitucional, de un derecho a la autodeterminación informativa. Los ciudadanos se ven obligados, por razones de interés general, a proporcionar una serie de datos relativos a su vida cotidiana, al Estado. Si bien esta finalidad aparece legítima para garantizar una buena administración, en ningún caso esta recogida masiva de datos de carácter personal, de una nación entera, puede ser desviada hacia otros fines, como es el caso del Censo Promocional". Propuesta de Proyecto de Ley por la que se modifica la Ley Orgánica 15/1999, de 13 de Diciembre de Protección de Datos de Carácter Personal, presentada en público por la Comisión de Libertades e Informática el día 1 de Diciembre de 2004 en la sede del Consejo Económico y Social. Madrid.

[177] "El 1 de octubre de 1998 entró en vigor en España el Convenio hecho en Bruselas el 26 de julio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol). Se pueden citar en aquel sentido los artículos: 7.3, 8.4, 9.1, 17.1, 19.3, y en especial el artículo 14, relativo al nivel de protección de los datos, y los artículos 23. 2. y 38.11, sobre las competencias de la autoridad nacional de control en materia de este convenio y la protección de los ciudadanos". LÓPEZ GARRIDO, D. Recurso de inconstitucionalidad contra los artículos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

personales, la ausencia de una acción judicial propia para el derecho fundamental que garantiza, etc. Y todo ello teniendo en cuenta que ya desde sus comienzos fue tachada de inconstitucional en dos de sus artículos[178]. También cabe destacar, como particularidad, la ausencia de Exposición de Motivos en la LOPD.

En cuanto al desarrollo de esta legislación orgánica, se había asumido el entonces vigente Real Decreto 994/1999, de 11 de junio, que aprobaba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal. Norma que se quedó desfasada enseguida pero que, a pesar de sus deficiencias, no sería actualizada hasta el 21 de Diciembre de 2007, cuando se aprueba el nuevo Reglamento de desarrollo de la LOPD[179], ya adaptado, con mayor o menor acierto y tras dos años de debates, a las necesidades prácticas de aplicación de la Ley Orgánica.

Este nuevo Reglamento vino a hacer una especie de compilación de los resultados de la experiencia práctica en la aplicación de la normativa de protección de datos, y de otras normas surgidas posteriormente, con repercusión directa en la LOPD[180], para que los sujetos obligados a cumplir con la normativa, conozcan la verdadera trascendencia práctica de esta materia, evitando su vulneración y, por ende, la imposición de graves sanciones.

Las carencias detectadas en la LOPD venían siendo objeto de estudio desde 2003, en la Agencia Española de Protección de Datos. El 30 de

[178] En el fallo de la STC 292/200: "Estimar el presente recurso de inconstitucionalidad y, en consecuencia: 1º Declarar contrario a la Constitución y nulo el inciso "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o" del apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. 2º Declarar contrarios a la Constitución y nulos los incisos "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas" y "o administrativas" del apartado 1 del artículo 24, y todo su apartado 2, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".

[179] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[180] "El reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia". Exposición de Motivos del Real Decreto 1720/2007, de 21 de diciembre.

Diciembre de 2005, remitió al Ministerio de Justicia un primer borrador que sirvió de base para el debate y discusión del proyecto que debería ser aprobado. En Noviembre de 2007, el Consejo de Estado emitió un Dictamen[181] en el que dejó constancia de las alegaciones y aportaciones de un gran número de entidades, públicas y privadas.

Se trataba de ofrecer una mayor seguridad jurídica a los responsables de los ficheros, detallando las medidas de seguridad aplicables a los supuestos de tratamiento de datos de carácter personal más habituales a lo largo de 158 artículos, respondiendo así también a los problemas más habituales, pero sin pretender ser exhaustivo en la consideración de toda la casuística posible. Más adelante se analizará el texto técnico de esta norma, sirva aquí mencionar la Exposición de Motivos, por cuanto destaca que la misma "nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo. Por tanto, se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema".

La última reforma de la normativa específica se produjo con la aprobación de la Ley 2/2011, de 4 de marzo, de Economía Sostenible, cuya Disposición Final Quincuagésima Sexta modifica sustancialmente el régimen sancionador de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).

Las principales novedades de la reforma se producen sobre los arts. 43, 44, 45, 46 y 49, y puede decirse que las más significativas son la previsión de una atenuación para las sanciones en función de los diferentes

[181] Referencia 1909/2007, Dictamen de 15 de Noviembre de 2007.

tipos de sanciones, y la previsión del "apercibimiento" como medida no sancionadora, excepcional y limitada, que pretende evitar la imposición de sanciones y promover la corrección de conductas.

Respecto de los criterios de atenuación de las sanciones[182], se introduce el criterio de la proporcionalidad como criterio general en la aplicación de las sanciones, que por ejemplo se cuantificarán en función del (artículo 45.4) "volumen de negocio o actividad del infractor", de "la diligencia profesional sobre el tratamiento de datos exigible al infractor"[183] o, si el infractor ha "regularizado la situación irregular de forma diligente"[184]. En éste último caso, pueden existir dificultades que impidan su consideración, puesto que sólo se podrá afirmar que existe una "situación irregular" cuando la Agencia así lo haya declarado, salvo que lo que se quiera promover la espontánea declaración de culpabilidad del expedientado.

Por otra parte, se introduce la figura del "apercibimiento" para aquellos infractores leves o graves no reincidentes (artículo 45.6), de forma que la Agencia Española de Protección de Datos podrá, de manera excepcional, no instruir el procedimiento sancionador cuando los hechos fuesen constitutivos de infracción leve o grave, si el infractor no hubiese sido sancionado o apercibido con anterioridad[185]. De no ser atendido este aviso, el

[182] Se han modificado los importes de las sanciones leves y graves (artículo 45.1 y 2): para las sanciones por infracciones leves, la multa va desde los 900 a 40.000 euros, y para las infracciones graves, desde de 40.001 a 300.000 euros.

[183] Artículo 45.4.i) de la LOPD, reformado – "La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor".

[184] Artículo 45. 5 de la LOPD, reformado – "El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos: a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo. B) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente. C) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción. D) Cuando el infractor haya reconocido espontáneamente su culpabilidad. E) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente".

[185] Artículo 45.6 de la LOPD, reformado – "Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos: A) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley. B) Que el infractor no hubiese sido sancionado o apercibido con anterioridad. Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera

procedimiento podrá continuar y, concluir con la imposición de la correspondiente sanción.

En general, según la Agencia Española de Protección de Datos, se pretende una "mejora de la tipificación de las infracciones vinculándolas a la vulneración de los principios específicos que garantizan la protección de datos personales, y que –por ejemplo- permitirán que las cesiones ilícitas de datos pasen a equipararse a otras infracciones graves como el tratamiento de datos sin consentimiento, equilibrando bienes jurídicos protegidos que estén incluidos en la misma definición de "tratamiento de datos". El tratamiento o la cesión de datos sólo se tipificarán como infracciones muy graves cuando afecten a datos especialmente protegidos. Del mismo modo se establece un régimen homogéneo y se armonizan las infracciones relativas al impedimento u obstaculización del ejercicio de los derechos recogiéndolos en un mismo tipo para todos ellos"[186]. Esta reforma pretende en definitiva aportar una "mayor seguridad jurídica y mayor precisión en la aplicación de la norma, aplicando los criterios de modulación y adecuación de las sanciones".

Además de la normativa especial expuesta, en materia de protección de datos existen otros textos legales de especial carácter que también han contribuido eficazmente a configurar el panorama legislativo español en esta materia que, habiendo sido promulgadas bien con anterioridad, bien con posterioridad a la LOPD, lo cierto es que están directamente conectadas por los preceptos que contienen sobre esta materia.

Anteriores a la LOPD, destacan, por cuanto continúan aún vigentes: La Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen; la Ley 26/1984, de 19 de julio, general para la defensa de los Consumidores y Usuarios; la Ley 9/1968, de 5 de abril, reguladora de los Secretos Oficiales;

---

determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento".

[186] Nota informativa de la AEPD, de 7 de marzo de 2011, sobre la modificación del régimen sancionador de la LOPD. Disponible en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2011/notas_prensa/common/marzo/NP_modificacion_LOPD.pdf

la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad; la Ley 12/1989, de 9 de mayo de la Función Estadística Pública; el Código Penal (Artículos relativos a delitos informáticos[187]); la Ley 34/1988, de 11 de noviembre, General de Publicidad; la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común; la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado (Disposición Adicional 10); la Ley 14/1986, de 25 de abril, General de Sanidad, la Ley 25/1990, de 20 de diciembre, del Medicamento; y la Ley 35/1988, de 22 de noviembre, sobre Técnicas de Reproducción Asistida

Y, posteriores a la entrada en vigor de la LOPD, existen normas de carácter sectorial, en las que la protección de datos personales adquiere gran relevancia:

- Ámbito Sanitario: la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; la Ley 16/2003, de 28 de marzo, de cohesión y calidad del Sistema Nacional de Salud; la Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesionales Sanitarias; la Ley 45/2003, de 21 de noviembre, por la que se modifica la Ley 35/1988, de 22 de noviembre, sobre Técnicas de Reproducción Asistida; y la Ley 3/2007, de 15 de marzo, reguladora de la rectificación registral de la mención relativa al sexo de las personas.

- Ámbito de la Firma electrónica: Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

- Ámbito de la Administración: la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos; y, la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

[187] Tener en cuenta la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. BOE. Nº. 152. Miércoles 23 de junio de 2010. Sec. I. p. 54811, en el que se modifican algunos artículos relativos a los delitos informáticos.

- Ámbito Financiero: la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero; la Ley 230/1963, de 28 de diciembre, General Tributaria (actualizada a 23 de mayo de 2003); y la Ley 58/2003, de 17 de diciembre, General Tributaria.

- Ámbito de las Telecomunicaciones: la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico; la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones[188]; la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones; y la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

- Ámbito de los Seguros: Ley 34/2003, de 4 de noviembre, de modificación y adaptación a la normativa comunitaria de la legislación de Seguros Privados; y, la Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros privados.

- Ámbito mercantil: Ley 29/2009, de 30 de diciembre, por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de la protección de los consumidores y usuarios.

- Ámbito de las Fuerzas y cuerpos de Seguridad: Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

De forma singular, debe incluirse en este apartado, una posibilidad que se recoge en la propia LOPD: la "autorregulación" a través de Códigos Tipo. Las empresas (grupos empresariales) y, cada vez más, se van dotando

[188] Modificada por el Proyecto de Ley, publicado en el Boletín Oficial de las Cortes Generales, Congreso de los Diputados, Serie A de 27 de mayo de 2011 (http://www.congreso.es/public_oficiales/L9/CONG/BOCG/A/A_124-01.PDF) Incorpora al ordenamiento jurídico interno las Directivas europeas de Mejor Regulación y de Derechos de los Ciudadanos, que junto al Reglamento del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) integran el Paquete Telecom aprobado en noviembre de 2009: "mejoran los derechos de los consumidores, garantizan un mejor acceso a Internet, protegen mejor los datos, impulsan la competencia y modernizan la utilización del espectro radioeléctrico. Asimismo se promueve la calidad de los servicios y la competencia entre operadores, incentivando la innovación y la inversión y creando un marco adecuado para el despliegue de redes de nueva generación".

de estos Códigos como normas de obligado cumplimiento, por acuerdos, en los que establecen pautas de comportamiento que habrán de seguirse en relación con el tratamiento de datos de carácter personal y, que se fundamentan en los mínimos que establece la LOPD. Esta solución al avance de la tecnología y el desfase que éste puede provocar en la regulación legal, pasa en todo caso por la supervisión y control de la Agencia de Protección de Datos y, está logrando que en los sectores que se acogen a esta forma de "autocontrol", se dé una mayor conciencia por la protección de los individuos en relación con el tratamiento de su información personal. "La autorregulación como un fenómeno característico del Estado de Bienestar, denota en puridad el "control jurídico" de la autorregulación social[189].

Este abanico normativo, en su efectivo ejercicio, ha dado lugar lógicamente a una prolija experiencia judicial reflejada en diferentes sentencias, que han contribuido decisivamente a esa delimitación de la protección de datos, tanto de su concepto como de su contenido. Y es que es tan importante la norma que recoge el derecho como la experiencia de su ejercicio, y de ahí que se deba dedicar un apartado a la jurisprudencia. La expresión "El derecho es mucho más complejo que las simples normas en las que se concreta"[190] comprende en pocas palabras que es necesario ir más allá de la positivación de las normas de comportamiento de la comunidad.

La labor integradora de la jurisprudencia respecto de los derechos fundamentales, tiene gran relevancia tanto para el significado más actual del derecho a la autodeterminación informativa, como para el desarrollo de sus garantías: Como se ha comentado ya, el interés doctrinal por la "libertad informática" se debió a fuentes del derecho anglosajón ("The Right to Privacy"), en relación con la informática, sin embargo el concepto "derecho a la autodeterminación informativa" surgió de la jurisprudencia, en concreto, de la jurisprudencia alemana.

---

[189] OLIVER LALANA, A.D., "Autorregulación, normas jurídicas y tecnologías de privacidad. El lado virtual del derecho a la protección de datos", en *XVII Encuentros sobre Informática y Derecho*, (2002-2003), Universidad Pontificia de Comillas (ICADE), Madrid, 2003. p. 96.

[190] MARTÍN RETORTILLO, S. *La doctrina del ordenamiento jurídico de Santi Romano y algunas de sus aplicaciones en el campo del Derecho administrativo.* (Estudio preliminar a la traducción de la obra de SANTI ROMANO, *El ordenamiento jurídico*). Instituto de Estudios Políticos. Madrid, 1963. p.35.

El proceso de configuración de este derecho como autónomo surge efectivamente para todo el ámbito europeo, con la Sentencia del Tribunal Constitucional Alemán, de 15 de diciembre de 1983, relativa a la Ley de censo de población. En ella se señalaba que, sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad, el tratamiento electrónico de datos personales suponía una injerencia en el derecho a la autodeterminación del ciudadano respecto a la transmisión de información personal. A pesar de que en la Ley Fundamental de 1.949 no existía, reconocido como tal, un derecho específico sobre el respeto a la información que caracteriza a los individuos, el Tribunal afianzó este aspecto de las libertades básicas, interpretando un nuevo instituto de garantía. En esta Sentencia el Tribunal Constitucional germano recoge la autodeterminación informativa como derecho específico, de dos artículos de la Ley Fundamental alemana[191]:

> 1. "En las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitadas de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2.º, párrafo 1, en relación con el artículo 1.º, párrafo 1, de la Ley Fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y la utilización de los datos referentes a su persona.
>
> *2.* Las limitaciones de este derecho a la "autodeterminación informativa" sólo son admisibles en el marco de un interés general superior" (...).

El párrafo primero del artículo primero ("Protección de la Dignidad Humana") dice textualmente que "la dignidad del ser humano es inviolable, y es obligación de todos los poderes estatales respetarla y protegerla" y, el párrafo primero del artículo segundo ("Derecho general de la personalidad

[191] De la traducción de la Sentencia publicada en el *Boletín de Jurisprudencia Constitucional*, Nº 33, 1984. p. 127.

propia") afirma que "todos tienen derecho al libre desarrollo de su personalidad, en tanto en cuanto no lesione los derechos ajenos y no contravenga el orden constitucional o las buenas costumbres". Concretamente este es el fundamento que justifica la garantía de la protección de datos de carácter personal del artículo 18.4 de la Constitución Española. El Tribunal Alemán señala que la proliferación de centros de tratamiento de datos y los avances tecnológicos posibilitan la producción de "una imagen total y pormenorizada de la persona respectiva -un perfil de la personalidad-, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en "hombre de cristal"[192]. Prioriza una nueva preocupación, los avances de la informática en relación con diferentes aspectos de la libertad y, sus efectos negativos sobre el individuo. En este contexto quedaría justificada por tanto la especial protección que se pueda dar a los derechos fundamentales para el ámbito virtual.

En España, fue fiel reflejo de esta situación el desarrollo positivo del artículo 18.4 de la CE, respecto de la garantía (la protección de datos de carácter personal) y, del artículo 10.1 CE, respecto del derecho en si y el entorno que lo justifica (el derecho a la dignidad).

La jurisprudencia española en esta materia, ha ido poniendo de manifiesto que la existencia de un derecho fundamental no está supeditada a que el mismo estuviese expresa y literalmente recogido con una concreta denominación pero, hasta llegar a esta afirmación, la jurisprudencia constitucional ha tenido que seguir un largo recorrido en el que no siempre se ha mostrado uniforme o, al menos, tan definido como aparece hoy[193]. El punto de partida no se centraba en el artículo 10.1 CE, para ponerlo en relación con los menoscabos provocados por la informática en los derechos fundamentales, si no que se centró en el derecho a la intimidad.

---

[192] *Boletín de Jurisprudencia Constitucional*, Nº 33. 1984. p. 137.

[193] "La falta de desarrollo legislativo del artículo 18.4 no puede implicar que el derecho fundamental a la protección de datos se convierta en un reconocimiento meramente teórico, sin ninguna relevancia práctica. Es necesario por tanto precisar el "mínimo contenido" del derecho fundamental a la protección de datos que opera sin desarrollo legislativo. Lo determinante es por tanto, fijar el contenido constitucional - las facultades – del artículo 18.4 CE, que debe tener aplicación directa e inmediata a partir de su positivación constitucional, sin estar supeditado al desarrollo legislativo". TRONCOSO, A. "La protección de datos personales: una reflexión crítica de la jurisprudencia constitucional". *Cuadernos de derecho público*, Nº 19-20. 2003 (Ejemplar dedicado a Protección de datos). p. 275.

En cuanto al concepto jurisprudencial del derecho a la protección de datos, la Sentencia 254/1993 del Tribunal Constitucional, de 20 de Julio, sobre el derecho al honor e intimidad, en su protección ante el uso de la informática y sobre los ficheros con datos personales[194], marca en España un punto de arranque en la delimitación de los elementos de este derecho, afirma que el derecho a la protección de los datos personales en muchos supuestos es un derecho instrumental del derecho a la intimidad o de otros derechos fundamentales, pero que es también un derecho o libertad fundamental en sí mismo[195].

El supuesto de hecho del que partió esta sentencia fue la denegación de acceso a una persona a los datos personales, de los que era titular, que constaban en los ficheros de las Administraciones Públicas. El Tribunal comienza la fundamentación jurídica señalando que "la cuestión suscitada en el presente recurso de amparo consiste en determinar si la negativa a suministrar la información solicitada, acerca de los datos personales del actor que la Administración del Estado posee en ficheros automatizados, vulnera o no los derechos fundamentales a la intimidad y a la propia imagen que le reconoce el artículo 18 de la Constitución, tanto en su apartado 1 como en el 4".(F.Jº. 1º).

Inicialmente el Tribunal considera el artículo 18.4 de la CE como la raíz de un derecho fundamental nuevo, al que atribuye una doble naturaleza, por una parte es un derecho fundamental y, por otra parte es también garantía de otros. Así, declara en su F.Jº. 6º que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos

[194] La STC 254/1993 se dictó con ocasión de un recurso de amparo interpuesto contra la denegación presunta por parte del Gobernador Civil de Guipúzcoa y del Ministro del Interior de la solicitud relativa a los datos de carácter personal existentes en ficheros automatizados de la Administración del Estado, confirmada en la vía contencioso-administrativa.
[195] TRONCOSO, A. "La protección de datos personales: una reflexión crítica … Op. Cit. p. 274.

fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática".

Sin embargo, aunque en una primera impresión puede parecer que efectivamente expresa que el artículo 18.4 es una garantía para la intimidad, y además, "es en sí mismo un derecho fundamental": "la libertad informática"[196], en el F.Jº. 7º, la sentencia de un giro de 180º para situar el núcleo del asunto en la vulneración del derecho a la intimidad a través de la denegación del acceso a la información personal. Explica en el F.Jº. 7º que se ha lesionado el derecho a la intimidad al no permitirse a la parte recurrida que hiciese efectivas "las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano, pues las considera absolutamente necesarias para que los intereses protegidos por el artículo 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos". Es evidente que en aquel momento para el Alto Tribunal, el derecho fundamental a la intimidad no agota su contenido en facultades puramente negativas, de exclusión, si no que "adopta un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)".

Parece que la argumentación jurídica pasa de entender el artículo 18.4 como el continente de un nuevo derecho fundamental, a entenderlo como una "extensión" del derecho a la intimidad[197].

---

[196] VILLAVERDE MENÉNDEZ, I., "Protección de datos personales, derecho a ser informado, y autodeterminación informativa del individuo. A propósito de la STC 254/1993", *Revista Española de Derecho Constitucional*, Mayo – Agosto, 1994. pp. 198 y ss. Se pronuncia este autor en desacuerdo sobre la interpretación que hace esta sentencia al entender que el artículo 18.4 CE supone la sede de un nuevo derecho fundamental.

[197] "No es ocioso advertir que a reciente aprobación de la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (LO 5/1992, de 29 de Octubre) no hace más que reforzar las conclusiones alcanzadas con anterioridad. La creación del Registro General de Protección de Datos, y

GÓNZALEZ MURÚA considera sobre esta argumentación que "un nuevo problema exige una nueva categoría jurídica"[198] y, que es posible que la intimidad, de los que configuran la dignidad del ser humano, sea el aspecto más vulnerable ante la informática. Pero admite que, a partir de lo expuesto del Tribunal Constitucional alemán, no todos los datos personales pertenecen a la esfera de lo íntimo. Sostiene en un principio la importancia de desvincular el derecho a la intimidad, del derecho a la protección de datos: "La estrecha conexión del derecho a la intimidad con la protección de los datos personales no se puede poner en tela de juicio, de hecho, la protección ante la informática arranca de este derecho. Sin embargo, en mi opinión (...) al ligar el derecho a la intimidad con la protección de los datos personales se ha producido una sustitución, (...) "por un concepto relacionado, pero distinto, cual es el ataque a la intimidad".

Esta autora consideraba dos derechos diferentes, pero uno como cimiento del otro. En aquel momento, la privacidad era punto de partida para la autodeterminación informativa y, así, afirma esta autora, de la STC 254/1993, que "se concluye que lo que el legislador llama privacidad viene a coincidir prácticamente con lo que se ha venido denominando por la doctrina autodeterminación informativa".

Esta conclusión no es aceptable hoy, la evolución jurisprudencial del concepto ha mostrado que, aunque el Tribunal Constitucional hiciese partir todos sus argumentos del derecho a la intimidad y, tratase de analizar los efectos del tratamiento de datos personales automatizado sobre este derecho, dejando de lado la idea de la autodeterminación informativa, el verdadero germen del derecho a la protección de datos personales fue éste, el derecho a la autodeterminación informativa.

---

el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, y además extienden su alcance a los de titularidad privada. Por ello no desvirtúa el fundamento constitucional de tales derechos, en cuanto a imprescindibles para proteger el "derecho fundamental a la intimidad" en relación con los ficheros automatizados que dependen de los poderes públicos. Ni tampoco exonera a las autoridades administrativas del deber de respetar ese derecho de los ciudadanos, al formar y utilizar los ficheros que albergan daros personales de éstos, ni del deber de satisfacer las peticiones de información deducidas por las personas físicas en el círculo de las competencias propias de tales autoridades". MARTINEZ MARTINEZ, R. *Una aproximación crítica* … Op. Cit., reproduciendo parte del F.Jº. 9º de la Sentencia.

[198] GONZÁLEZ MURÚA, A. R. "Comentario a la STC 254/1993, algunas consideraciones en torno al artículo 18.4 CE y la protección de los Datos Personales", en *Informática y derecho: Revista iberoamericana de derecho informático*, nº 6-7. 1994. pp. 242 y ss.

Para continuar dando forma a los elementos de este derecho a la autodeterminación informativa, la STC 143/1994 sigue a la anterior en su defensa del derecho a la intimidad como bien jurídico que proteger, aunque precisa que lo hace sobre el aspecto positivo (no íntimo). Sorprende la forma de expresarlo en la afirmación contenida en su F.Jº. 6º que determina que dada "la conexión necesaria que ha de existir entre el derecho en cuestión y la esfera reservada para sí por el individuo, en los más básicos aspectos de su autodeterminación como persona, resulta, por lo menos, cuestionable que en abstracto pueda entenderse vulnerada su intimidad por la exigencia de transmitir información sobre actividades desenvueltas en el tráfico económico y negocial. Unas actividades que tienden a desarrollarse 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".

El Tribunal distingue entre la esfera reservada o íntima y, lo que son los datos de carácter personal. En principio les asigna a éstos una esfera más amplia, que parece incluso independiente pero, más adelante lo desvirtúa. En el F.Jº. 7º, basándose en la anterior Sentencia, dice que "se hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto, que produzca este efecto, y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho (STC 254/1993). En este sentido se ha afirmado que, ya que "los datos personales que almacena la Administración son utilizados por sus autoridades y servicios", no es posible "aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión". También en este fundamento jurídico reconoce que: "un sistema normativo que, autoriza la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluye garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera

en que lo harían las intromisiones directas en el contenido nuclear de ésta"[199].

Otra sentencia similar, dictada cuatro años más tarde en relación con un asunto que afectó a la compañía ferroviaria R.E.N.F.E, fue la STC 11/1998. En aquel momento se dictaron una serie de sentencias[200] siguiendo similar línea jurisprudencial, y esta fue la que afirmó con mayor rotundidad la existencia de un derecho nuevo en el artículo 18.4 de la CE. Retomaba en general los argumentos de la STC 254/1993 ya señalados respecto del derecho a la intimidad y además, materializaba el carácter de derecho instrumental del artículo 18.4 de la CE para la protección de otros derechos. En este caso concreto se resuelve sobre la vulneración de la libertad sindical como consecuencia de la utilización ilegítima de los datos personales contenidos en una base de datos informatizada. Señala en su F.Jº. 4º que "dicho precepto (el artículo18.4 CE) incorpora una garantía constitucional, para responder a una nueva forma de amenaza concreta a la dignidad y los derechos de la persona. Además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en si mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso legítimo del tratamiento mecanizado de datos. La garantía de la intimidad, latu sensu, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención". Concluye pues que el artículo 18.4 de la CE es un derecho fundamental y también, una garantía. Se trata del derecho a ser protegido frente a las intromisiones de la informática en la esfera

[199] En el mismo sentido, STC 94/1998 (F.Jº. 4º).

[200] Se dieron en poco tiempo una serie de sentencias, todas ellas relacionadas con la informática y su potencialidad lesiva frente al derecho de libertad sindical. Son las SSTC 11/1998, 33/1998, 35/1998, 45/1998, 60/1998, 77/1998, 94/1998, 104/1998, 105/1998, 106/1998, 123/1998, 124/1998, 125/1998, 126/1998, 158/1998, 198/1998 y 223/1998. En la primera, la STC 11/1998 se resuelve sobre la utilización por RENFE de un fichero de datos sobre afiliación sindical para elaborar una relación de trabajadores pertenecientes a determinado sindicato que había convocado una huelga, con la intención de recortarles el salario en la proporción correspondiente a la duración de aquélla.

personal, a través del tratamiento automatizado de la información característica del individuo y, de la garantía que conlleva el mero hecho de estar previsto por la CE, para exigir el respeto de otros derechos como la intimidad frente a este tipo de "agresiones".

Por tanto, la aportación que hace esta sentencia es la de considerar que no es únicamente la intimidad lo que protege el artículo 18.4 de la CE, sino que la informática puede menoscabar otros aspectos diferentes de la libertad y dignidad humana[201].

Es también esta sentencia la primera que introduce el término "privacidad" respecto a la protección de datos, al aludir[202] a la Exposición de Motivos de la derogada Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal (LORTAD). Al citar este texto, pone el dedo en la llaga al decir que se "consagra" un derecho fundamental autónomo "a controlar el flujo de informaciones que conciernen a cada persona", pertenezcan o no al ámbito más estricto de la intimidad aunque, enseguida retoma la expresión "libertad informática" en conexión con la citada dimensión positiva del derecho a la intimidad.

Parece que con estas afirmaciones se va confirmando la intención de instaurar un nuevo derecho fundamental, parece que el Tribunal lo crea "ex novo", como así lo han considerado diferentes autores[203] e incluso se insinúa

[201] "Llama la atención que el ponente de la Sentencia 143/1994, de 9 de mayo, es el Magistrado Rodríguez Piñeiro, que emitió un voto particular en la Sentencia 254/1993, de 20 de Julio, antes analizada. Este Magistrado, aprovecha la ponencia para evitar la afirmación del derecho fundamental a la protección de datos personales como derecho autónomo del derecho a la intimidad. Lo que hace es interpretar el derecho a la intimidad a partir de las necesidades que se derivan de la informática, apoyándose en el Convenio 108, que se interpreta a la luz del derecho fundamental a la intimidad. La Sentencia no realiza esfuerzo alguno por completar e integrar el contenido del artículo 18.4 CE con el Convenio 108 por la vía del artículo 10.2 CE". TRONCOSO, A. "La protección de datos personales: una reflexión crítica … Op. Cit. p. 280.

[202] STC 11/1998 (F.Jº. 5º). "En suma, ha de concluirse que tuvo lugar una lesión del artículo 28.1 en conexión con el artículo 18.4 CE. Este no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad según la expresión utilizada en la E. de M. de la LORTAD-, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos".

[203] GONZÁLEZ MURÚA, A.R., sigue también esta tesis en su artículo "Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4º de la Constitución y la protección de datos", *Revista Vasca de Administración Pública*, núm. 37, 1993, pp. 227 - 270. Más adelante, esta autora escribió un nuevo artículo "Algunas Reflexiones en torno al artículo 18.4 de la Constitución y la protección

en alguna sentencia del Alto Tribunal, como la Sentencia 290/2000[204], de 30 de noviembre de 2000.

Sin embargo, el término "consagrar" sólo puede entenderse en el sentido de reafirmar la existencia previa de un derecho fundamental concreto, contenido en la redacción del artículo 10.1 CE y, cuyo núcleo es desvelado por el Tribunal Constitucional a través de las argumentaciones jurídicas de su jurisprudencia. No se admite por tanto la propuesta de la existencia de un instituto-garantía e instituto-derecho a la vez, integrado en un único precepto constitucional. La idea opuesta, de que "la inexistencia de una categoría constitucional específica no implica que el Tribunal deba limitarse a una interpretación del derecho a la intimidad en su concepción más tradicional como libertad negativa que no comporta, salvo que el legislador expresamente lo disponga, facultades positivas de actuación (...) el Tribunal puede buscar y ha buscado una interpretación de las normas acorde con la realidad social del tiempo en que las han de ser aplicadas"[205], ofrece un punto de vista más acertado, por cuanto acepta la posibilidad de que un precepto constitucional contemple con su enunciado la configuración de más de un derecho fundamental, como es el caso del artículo 10 de la CE.

Otra resolución que contribuye a la configuración del derecho a la protección de datos, es la STC 144/1999, de 22 de Julio, relativa a la solicitud de datos de antecedentes penales que realiza el Presidente de la

---

de los datos personales", en la publicación *Informática y Derecho*, Mérida, España, Universidad Nacional de Educación a Distancia (UNED), No. 6-7, 1994, pp. 242 y ss., dónde siguiendo las tesis de LUCAS MURILLO DE LA CUEVA conviene en la ruptura del binomio intimidad – protección de datos personales, pero, dice también que "como acertadamente señala Lucas Murillo de la Cueva, "basta con repasar los preceptos de la Constitución de 1978 para comprobar que entre los derechos que en ella se enuncian no figura ninguna denominado "derecho a la autodeterminación informativa". Sí encontramos, en cambio, tanto en el artículo 18.1 como en el 18.4 la mención del derecho a la intimidad personal y familiar. Por su parte, este autor no pone en tela de juicio la estrecha conexión de este nuevo derecho con el ya conocido derecho a la intimidad, es más se apresura y adelanta que el derecho a la autodeterminación informativa se construye a partir de la noción de intimidad" (p. 250).

[204] Sobre el contenido de esta sentencia, señala el magistrado del Tribunal Superior de Justicia de Andalucía, Alfonso Martínez: "Se trata, sin duda, de la formulación de un derecho nuevo o, al menos, de contenido sui generis (...) con ello el Tribunal reconoce y protege ahora un derecho fundamental, el derecho de libertad informática, que no figura explícitamente en la Tabla del texto de 1978, planteando así otros interesantes temas, como el carácter abierto o cerrado de la norma constitucional y si los Tribunales, tanto los ordinarios como el constitucional, deben extender la tutela a determinadas zonas del Derecho no expresamente consideradas en las correspondientes Constituciones, cuando es necesario hacerlo para que no queden a la intemperie, sin techo jurídico alguno, intereses esenciales de los ciudadanos". MARTÍNEZ ESCRIBANO, A. "Los derechos fundamentales y las nuevas tecnologías en el trabajo". *Revista Deliberación*, de la Asociación Profesional de la Magistratura, Nº 3, Junio 2002. Disponible en: http://www.apmagistratura.com/apm/deliberacion/admjus01.htm

[205] MARTÍNEZ MARTÍNEZ, R. *Una aproximación crítica…* Op. Cit. p. 306.

Junta Electoral de Zona de Santander, de 26 de Mayo de 1995, y que le fueron remitidos contra la voluntad (consentimiento) del recurrente. En los fundamentos de derecho, esta resolución analiza la tutela del derecho a la intimidad reconducido a la protección de datos. Sus argumentos se basan en que se puede aplicar a la protección del derecho a la intimidad, los principios del derecho a la protección de datos personales, en la medida que exista una intromisión en la vida privad. Afirma que "inicialmente pueden quedar excluidos de ese poder de disposición aquellos datos o informaciones producidos y destinados al tráfico jurídico con terceros o sometidos a fórmulas específicas de publicidad (SSTC 110/1984, 143/1994), pero no lo es menos que esta circunstancia no obsta para que el individuo esgrima un interés legítimo en sustraerlos del conocimiento de los demás, como del mismo modo lo puede haber para que esos aspectos de la vida individual sean públicos y conocidos, o puedan serlo (ATC 877/1987). Y ello es así porque el artículo 18.1 C.E. no garantiza sin más la "intimidad", sino el derecho a poseerla, a tener vida privada disponiendo de un poder de control sobre la publicidad de la información relativa a nuestra persona y familia, sea cual sea el contenido de aquello que se desea mantener al abrigo del conocimiento público. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías, y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información"[206]. La Sentencia amplía el contenido clásico del derecho a la intimidad, extendiéndolo hacia el control sobre la información personal, y dando la razón al recurrente sobre los límites de la actuación del Registro Central de Penados y Rebeldes, en los supuestos de acceso legítimo a sus datos (es precisa una habilitación legal expresa).

[206] STC144/1999, de 22 de Julio. F.Jº. 8º. (...) "constituyendo una ilegítima intromisión en la intimidad individual, lesiva del artículo 18.1 C.E. la infracción de las normas sobre acceso a la información relativa a una persona o su familia, con independencia de que esa información sea objetivamente considerada de las íntimas o de que su conocimiento o divulgación pueda ser perniciosa para la integridad moral o la reputación de aquel o de aquellos a quienes se refiere. Pues, de no ser así, atribuiríamos a los poderes públicos el poder de determinar qué es íntimo y qué no lo es, cuando lo que el artículo 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio".

La STC 202/1999, de 8 de noviembre, dictada en relación con la utilización de los datos de carácter personal relativos a la salud de los trabajadores de una empresa, que fueron recabados con el fin de preservar su salud pero, que realmente fueron integrados en una base de datos con fines de control laboral del absentismo con baja médica. En este contexto, el Tribunal Constitucional entró a decidir respecto de la esfera reservada de la personalidad (de datos de carácter reservado), ligándola al derecho a la intimidad. Comienza la sentencia argumentando el derecho a la intimidad y, concluye también citando el "instituto de garantía de otros derechos, fundamentalmente el honor, la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental", de tal forma que en este caso, es más fácil incurrir en confusiones, por cuanto se habla de "reservado". Este es un concepto estrechamente relacionado con el ámbito privado de la persona (F.Jº. 1º), es decir, con la esfera de la intimidad. Insiste por tanto en la idea de que el derecho de control sobre los datos relativos a la persona es la garantía positiva del derecho a la intimidad, manteniendo con ello la contradicción que representa el hablar de un nuevo instituto mientras que, por otro lado, lo contempla como incluido en el derecho a la intimidad.

En ese mismo año, la aparición de la Ley Orgánica de 15/1999 de Protección de Datos de Carácter Personal provoca que, a iniciativa de la Comisión de Libertades e Informática[207], Diego López Garrido, Diputado y Secretario General del Partido Democrático de la Nueva Izquierda en aquel momento, redacte el dictamen jurídico que sirvió de base al Recurso de Inconstitucionalidad presentado ante el Defensor del pueblo en febrero del año 2000 y, que tenía por objeto la declaración de diferentes preceptos como contrarios a la Constitución[208]. El resultado fue la STC 292/2000, y con ella,

[207] Asociación sin ánimo de lucro, dedicada a preservar el contenido esencial del derecho a la protección de datos en el territorio nacional.

[208] De la redacción literal del citado Recurso: "Por todas las razones expuestas, consideramos que los siguientes preceptos de la Ley Orgánica 15/1999 son contrarios a la Constitución:
1) el artículo 2.2.c)
2) el artículo 4.2
3) el artículo 7.6
4) el artículo 21.1
5) los artículos 22.2 y 3 y 23.1
6) los incisos "funciones de control y verificación de las Administraciones Públicas" y persecución de infracciones "administrativas" del artículo 24.1
7) el primer párrafo del artículo 24.2

un antes y un después en materia de intimidad y protección de datos[209]. Esta es la sentencia que va a consolidar definitivamente el originario derecho a la autodeterminación informativa como un derecho autónomo e independiente[210] del derecho a la intimidad, y para cuya garantía se prefiere la denominación "protección de datos de carácter personal".

Además de que el fallo de la sentencia consideraba inconstitucionales dos puntos concretos de la Ley[211], su importancia realmente trascendió por la inclusión de afirmaciones indicadoras del cambio que estaba a punto de sucede en cuanto a lo que debe significar el derecho a la protección de datos así, dice en el F.Jº. 5º que "el artículo 18.4 CE fue esgrimido por primera vez en el caso de un ciudadano a quien le denegó el Gobierno Civil de Guipúzcoa información sobre los datos que sobre su persona poseía, resuelto por la STC 254/1993, de 20 de julio. Y lo dicho en esta pionera Sentencia se fue aquilatando en las posteriores". Estas sentencias y la opinión que les merecía el precepto 18.4 de la CE como instituto garantía y/o derecho[212], son pues el origen de esta afirmación pero, se dice además que este "derecho

---

8) el artículo 28.4
9) el artículo 31 y la Disposición Transitoria Segunda
10) la Disposición Adicional Sexta"

[209] Esta sentencia se analiza en conjunto con la Sentencia 290/2000, de 30 de noviembre de 2000 del Tribunal Constitucional, que resuelve sobre recursos de inconstitucionalidad contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, pero que por estar ya derogada, no trataremos en esta exposición.

[210] Según LUCAS MURILLO DE LA CUEVA, P. ,"su aspecto más destacado es, ni más ni menos, que da carta de naturaleza en nuestro ordenamiento jurídico a un nuevo derecho fundamental: el derecho fundamental a la protección de datos", de su artículo La primera jurisprudencia sobre el derecho a la autodeterminación informativa, *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid,* Nº 1. Marzo 2003. www.datospersonales.org

[211] La STC 292/2000 estimó el recurso de inconstitucionalidad y, en consecuencia, declaró contrario a la Constitución y nulo el inciso "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o" del apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Asimismo declaró contrarios a la Constitución y nulos los incisos "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas" y "o administrativas" del apartado 1 del artículo 24, y todo su apartado 2, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[212] STC 292/2000 (F.Jº. 5º) "Pues bien, en estas decisiones el Tribunal ya ha declarado que el artículo 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (F.Jº. 6º, reiterado luego en las SSTC 143/1994, F.Jº. 7º, 11/1998, F.Jº. 4º, 94/1998, F.Jº. 6º, 202/1999, F.Jº. 2º). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (artículo 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, F.Jº. 5º, 94/1998, F.Jº. 4º)".

fundamental a la protección de datos, a diferencia del derecho a la intimidad del artículo 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (artículo 81.1 CE), bien regulando su ejercicio (artículo 53.1 CE)".

En el fundamento jurídico siguiente (F.Jº. 6º), la resolución se pronuncia sobre cuál es la función del derecho fundamental a la intimidad del artículo 18.1 de la CE, "la de proteger frente a cualquier invasión que pueda realizarse en aquel 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 (por todas STC 144/1999, de 22 de julio, F.Jº. 8º). En cambio, el derecho fundamental 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 (...). El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado (...), y además 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, que no se contienen en el derecho fundamental a la intimidad".

Continuando en su exposición la Sentencia se pronuncia también sobre lo que debe ser su contenido concreto (F.Jº. 7º), y dice que los "poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y

tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos".

Es una trascripción literal de los párrafos más relevantes para la determinación del contenido del "derecho fundamental a la protección de datos", con la intención de mostrar la razón de ser que en ese momento le confiere el Tribunal Constitucional al artículo 18.4 de la CE como independiente del derecho a la intimidad. Estos argumentos no significan la determinación de un nuevo derecho, sino que se limitan a mostrar el contenido de un derecho fundamental concreto hasta ahora ignorado (no inexistente) y, lo hace partiendo de la garantía constitucional prevista, respecto de un entorno especialmente problemático o peligroso como es el ámbito de la informática. El artículo 18.4 de la CE protege la libertad informática y, según el Alto Tribunal, esto se traduce en que las personas tienen derecho a proteger sus datos de carácter personal. En este sentido, cabe pues plantearse que obviamos el ámbito de la tecnología, ¿no existiría el derecho a la protección de la información personal? En efecto, existiría, y ello porque no estamos ante un derecho que nace a la luz de las lesiones que provoca la informática en el ámbito de la intimidad, sino más bien, que este supuesto de hecho es el que pone de manifiesto su existencia y, con ello, la necesidad de otorgarle protección especial frente a los avances tecnológicos[213].

[213] "No obstante, hay que señalar que de la ubicación en el artículo 18 y de la propia mención expresa en el apartado 4 al derecho a la intimidad personal y familiar se desprende que el derecho a la protección de

Como se ha venido defendiendo, un derecho fundamental no tendría razón de ser si no conlleva su efectiva realización en la práctica, es decir, si no se conocen los elementos precisos de su contenido. A lo ya expuesto, han contribuido de forma complementaria distintas Sentencias de la Audiencia Nacional y del Tribunal Supremo[214], y con lo que se expone a continuación, se pretende transmitir la idea de que el ejercicio del derecho a la protección de datos personales requiere que observar un elenco específico de derechos, que deben asistir a los interesados ("haz de facultades"[215]) y, que van más allá de la mera realización de la intimidad (o incluso "privacidad").

Considerar que existe una especie de "Habeas Data para definir las garantías que deben asistir a los titulares del derecho a la protección de datos, facilita entender que la normativa vigente[216] recoge un haz de facultades o derechos que lo hacen realizable: los derechos de información, de acceso, de rectificación, cancelación, oposición e información. Estos, junto con requisitos como la información o el consentimiento para el tratamiento de datos de carácter personal, serán el objetivo de su protección, y serán por tanto el núcleo de múltiples resoluciones judiciales dictadas sobre diferentes circunstancias en se han venido suscitando los conflictos de su aplicación.

En el orden jurisdiccional, los órganos fiscalizadores de esta materia son, tras la entrada en vigor de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-administrativa, las Salas de lo Contencioso-administrativo de la Audiencia Nacional[217]. Con anterioridad a la promulgación de esta Ley, podían conocer de estos asuntos los Tribunales

---

datos personales no debe ser visto como un derecho absolutamente independiente, sino dentro de la esfera amplia del derecho a la intimidad, como una especie de manifestación más de la protección de la vida privada, aunque tutele también el ejercicio de otros derechos fundamentales – como, por otra parte, también le ocurre al propio derecho a la intimidad –. El derecho a la protección de datos personales representa, de alguna manera, una concretización del derecho a la intimidad en los tratamientos de datos personales, una actualización del derecho a la privacidad frente al desarrollo de las tecnologías de la información, un derecho más específico dentro del más general derecho de privacidad personal". TRONCOSO, A. "La protección de datos personales: una reflexión crítica … Op. Cit. pp. 321 y 322.

[214] Los textos completos de las sentencia que aquí se citan se pueden consultar en: www.agpd.es

[215] Ibídem (F.J. 5º).

[216] La normativa específica se analizará en un momento posterior con detalle.

[217] Tras la entrada en vigor de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-administrativa, se atribuyó definitivamente el conocimiento de este tipo de asuntos a Audiencia Nacional. Disposición Adicional Cuarta. Recursos contra determinados actos, resoluciones y disposiciones, apartado 5º: "Los actos administrativos dictados por la Agencia de Protección de Datos, Comisión del Sistema Eléctrico Nacional, Comisión del Mercado de las Telecomunicaciones, Consejo Económico y Social, Instituto Cervantes, Consejo de Seguridad Nuclear y Consejo de Universidades, directamente, en única instancia, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional".

Superiores de Justicia y, se citan a modo de ejemplo, la Sentencia dictada el Tribunal Superior de Justicia de Andalucía, con fecha de 5 de febrero de 1991 y la Sentencia del Tribunal Superior de Justicia de Galicia, de 31 de mayo de 1996. Ambas mostraban ya el carácter instrumental del artículo 18.4 de la CE en relación con el concreto derecho a la libertad sindical, consideraron que la utilización del dato "afiliación" para comunicar a los representantes sindicales, el despido de éste, supone la utilización de este dato para un fin compatible con el que motiva el tratamiento, por tanto dicha utilización es conforme a lo dispuesto en la Ley Orgánica 15/1999. Sin embargo se analizaba en el fondo, el papel de la finalidad del tratamiento de los datos de carácter personal, en este caso, sobre una esfera no íntima del trabajador. En aquel momento, la jurisprudencia constitucional mantenía aún la dependencia de la autodeterminación informativa y la intimidad, y sin embargo, resolvió de conformidad con el deslinde de ambos, ya que de lo contrario, el dato "afiliación sindical" se habría considerado parte de la esfera íntima del trabajador y, con ello, indisponible para terceros sin el consentimiento del afectado.

Otra sentencia que requiere ser mencionada es la que se dictó sobre un recurso interpuesto en 1997 frente a una resolución[218] de la autoridad encargada de velar por la defensa del derecho fundamental a la protección de datos, frente a la Agencia de Protección de Datos. La resolución, dictada con fecha 16 de Julio del año 2002 por la Sala de lo Contencioso-administrativo del Tribunal Superior de Justicia de Madrid, sentenció que para poder realizar transferencias de datos personales entre empresas, era necesario el consentimiento informado del titular de los mismos (F.Jº. 5º), pues se crearía un peligro añadido de no hacerse así, el de la realización de perfiles de las personas. Una vez más, se muestra la creciente preocupación por la observancia de los elementos del contenido esencial de este derecho, para poder ver su ejercicio efectivamente realizado, en este caso, la información y el consentimiento.

[218] Resolución AEPD, de 6 de junio de 1997, en que se sancionaba a una empresa filial de un determinado operador de telecomunicaciones.

Ya en el entorno de las decisiones de la Audiencia Nacional, la extensa jurisprudencia generada nos exige a los efectos de esta exposición escoger de entre todas las resoluciones algún ejemplo concreto que pueda mostrar otros elementos que, en el ejercicio del derecho a la autodeterminación informativa, se hayan visto en conflicto.

Así, se pueden destacar respecto del consentimiento y la importancia de su carácter de inequívoco, según la Ley Orgánica 5/1992, las Sentencias número 103/1999, de fecha 14 de abril de 2000 y, la número 121/1999, de 7 de julio de 2000. La primera, en su F.Jº. 7º señaló que "tampoco puede admitirse (...) la existencia de un consentimiento tácito o impropiamente llamado "silencio positivo" del afectado para admitir la cesión de sus datos, pues tal forma de obtener el consentimiento requeriría, en la mejor de las hipótesis, una rigurosa constancia documental de que la entidad cedente había informado y conservaba el escrito, con constancia de la recepción por el interesado". La segunda sentencia, en su F.Jº. 3º explica, respecto del sistema para recabar los datos de clientes y cederlos posteriormente, que se realizaba a través de "comunicación remitida a todos por vía ordinaria advirtiéndoles que de no mediar oposición expresa, se considerarían legitimadas para la cesión. Este tema del consentimiento tácito ha de ser tratado con una gran delicadeza cuando están en juego derechos constitucionales básicos, (artículo 18.4 C.E.) y a ello tiende toda la regulación legal contenida en el articulado de la L.O. 5/92 y su explicación y filosofía recogida en la Exposición de Motivos". Remarcando la importancia de entender el adjetivo "tácito", como límite al contenido del derecho en cuestión, señala esta sentencia que en la vida "es muy posible reconocer formas de tácita aceptación, pero siempre en aspectos no trascendentales o cuando se está operando sobre situaciones consolidadas y que están en la común consideración a modo de valores entendidos. No es el caso cuando lo que está en juego es la privacidad de las personas de ahí todas las cautelas normativas tendentes a proteger esa privacidad, sin que quepan interpretaciones de laxitud del artículo 11.1 de la Ley a menos que el titular de la intimidad se haya situado voluntariamente en situación de abandono de la defensa de ese derecho, en cuyo caso sí podría hablarse de una forma de consentimiento tácito. Pero hay más, y es que ni tan siquiera consta que los

denunciantes hayan recibido ninguna comunicación que se dice hecha por correo ordinario y cuya recepción se niega e incluso de ser cierta sería más que dudosa su eficacia sustitutoria del consentimiento".

Dos importantes conclusiones se pueden extraer de estas Sentencias, la primera es que el criterio que establecían respecto a lo que se debía entender como tácito, se elaboró teniendo en cuenta que el consentimiento es un elemento esencial para la garantía de la protección de datos personales[219], y que debe ser especialmente observado cuando su inexistencia pueda además poner en peligro la intimidad de las personas.

Relevante también es la Sentencia de la Audiencia Nacional, de 11 de febrero de 2004 (Recurso núm. 132/2002), que confirmó una sanción impuesta por la Agencia Española de Protección de Datos (sanción de 420.708,47 euros) a Telefónica de España, S.A., por haber tratado datos personales que poseía, para fines distintos de los propios del suministro del servicio de telefonía y su posterior facturación. El fallo se basaba en la aplicación del principio de la finalidad al tratamiento de los datos de carácter personal. El artículo 4 de la LOPD cita que no se pueden utilizar los datos con fines "incompatibles" con aquellos para los que se recabaron, sin embargo esta Sentencia juega con el término "distintos", término que salvo mejor opinión en derecho debió adoptar la LOPD desde un primer momento.

Por otra parte, el consentimiento del afectado normalmente se recaba respecto de unos datos concretos y sólo para el tratamiento de éstos, su uso por tanto habrá de circunscribirse también al límite específico de la calidad de los datos.

[219] Este criterio, no se sigue ya hoy estrictamente por la Agencia Española de Protección de Datos. Así lo ha expuesto en sendas Resoluciones de Archivo de Actuaciones sobre las denuncias interpuestas por diferentes asociaciones, particulares y entidades privadas, contra los procedimientos que habitualmente vienen utilizando las operadoras de telefonía Telefónica S.A. y Amena (del grupo Retevisión Móvil S.A.) para proceder a la utilización de los datos de sus clientes con fines de marketing, sin necesidad de un consentimiento "inequívoco". La primera resolución, sobre la actividad de Telefónica S.A es de fecha 11 de febrero de 2005, y la segunda, sobre Amena, de 7 de Junio del mismo año, en ambas la Agencia Estatal de Protección de Datos resuelve la situación explicando que dichas entidades privadas tienen la carga de la prueba a la hora de demostrar que los derechos de los ciudadanos no se han visto cercenados por desconocer que se estaban tratando así sus datos de carácter personal, sin querer entrar a ver si el propio procedimiento suponía de por sí dicho cercenamiento, tal y como expresa la sentencia a que se refiere la presente cita.

Éste es otro importante principio rector de la materia de protección de datos, y ha tenido un reiterado referente de aplicación en el supuesto de las listas de morosos y la inclusión de particulares en ellas. La Sentencia de de la Audiencia Nacional 1144/1999, de fecha 16 de febrero de 2001, señaló en su F.Jº. 4º que el uso de "unos datos relativos a la insolvencia de una persona, conculcando los principios y garantías establecidas en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento de Datos de Carácter Personal, concretamente el de la certeza de los datos, que deben ser exactos, de forma que respondan con veracidad a la situación real del afectado, como exige su artículo 4.3 (...) ha de decirse que la inclusión equivocada o errónea de una persona en el registro de morosos, es un hecho de gran trascendencia de la que se pueden derivar consecuencias muy negativas para el afectado, en su vida profesional, comercial e incluso personal, que no es necesario detallar. En razón de ello, ha de extremarse la diligencia para que los posibles errores no se produzcan, cerciorándose previamente si la persona deudora es realmente aquella cuyos datos se facilitan a dicho registro".

Habiendo visto cómo se refleja jurisprudencialmente el artículo 18.4 de la CE, y sus elementos esenciales tales como la "información" y el "consentimiento", o el principio de la calidad de los datos para su tratamiento, corresponde ahora analizar más en detalle la consideración jurisprudencial de los derechos de acceso, rectificación y cancelación, elementos también del haz de facultades que componen ese derecho.

Sobre el derecho de rectificación sirve como ejemplo a los efectos de esta exposición la resolución ya mencionada sobre los listados de morosos y la calidad de los datos, pues para poder mantener la calidad de los mismos, su rectificación para ser actualizados puede darse de oficio, por la entidad responsable del fichero o bien, a petición de parte interesada. La Audiencia Nacional se ha pronunciado sobre este elemento más recientemente en las Sentencias de fecha 10 de mayo de 2002, sobre conservación de datos de obligaciones satisfechas en ficheros de solvencia patrimonial y crédito ("Saldo cero") y, de fecha 8 de octubre de 2003, sobre la responsabilidad por incluir datos inexactos en ficheros sobre solvencia patrimonial y de crédito.

Respecto del derecho de acceso, se puede citar como ejemplo la Sentencia de la Audiencia Nacional de 26 de junio de 2003, relativa a los ficheros de publicidad y prospección comercial. Esta sentencia confirma una sanción impuesta desde la Agencia de Protección de Datos por una infracción del derecho de acceso regulado en el artículo 15 de la LOPD y, de otra parte, una sanción por la infracción del artículo 5.4 de la LOPD, por no haber informado al interesado del origen de los datos. Sobre el derecho de cancelación, puede verse la Sentencia de la Audiencia Nacional, de fecha 16 de Febrero de 2001, por la que se resolvía el recurso de un laboratorio que contrató una campaña publicitaria para un producto y creó para ello una base de datos, uno de los destinatarios del envío publicitario, ejercitó su derecho de cancelación frente al laboratorio y éste se lo denegó, alegando que no constaba en sus archivos. Se demostró que el laboratorio había mantenido datos del afectado en contra de su voluntad, y se resolvió estableciendo la vulneración de este derecho previsto por la LOPD. Y, por último, sobre la obligación de observar las medidas de seguridad adecuadas, elemento más práctico de la garantía que además es imprescindible para la efectiva existencia de todo lo demás, se cita tan sólo a modo de ejemplo, la Sentencia de fecha 13 de Junio de 2002, sobre la vulneración del deber (de seguridad) de conservar cierta documentación que debió ser cancelada o destruida.

Significativas son también las sentencias dictadas por el Tribunal Supremo resolviendo recursos de casación, bien para la unificación de la doctrina, bien resolviendo impugnaciones de otras sentencias dictadas por los Órganos Judiciales. Una de las primeras que se dictó en esta materia por el Tribunal Supremo, fue la Sentencia de 28 de octubre del año 2000, de la Sala de lo contencioso-administrativo (Sección sexta), que resolvió sobre la determinación del tipo infractor, según se tenga conocimiento previo o no de la inexactitud del dato y, sobre la necesidad de unificar la doctrina por existir una contradicción entre la sentencia recurrida y la anterior sobre dicho tipo. Esta sentencia declaró no haber lugar al recurso de casación debido a que la sentencia recurrida se resolvió de modo ajustado a Derecho[220] sobre cuál era

[220] Se señala en su F.Jº. 6º que: (...) "en los supuestos resueltos por una y otra sentencia de la Sala de instancia con diferentes pronunciamientos, pero mientras que la doctrina mantenida en la primera

el tipo. Se entendió que no conocer la inexactitud de un dato no era excusa para no mantener actualizado en un registro o fichero con datos de deudores.[221] A esta sentencia le siguieron otras también en materia de unificación de doctrina, como la dictada el 12 de abril del año 2002, que invocaba la aplicación del artículo 45.5 LOPD sobre "la apreciación de una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, por el que el órgano sancionador debía establecer la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate"[222].

Otras sentencias, desestimaron los recursos que las originaron, por no apreciarse la concurrencia de los requisitos formales relativos al proceso y a la resolución que se aludían para recurrir, son: la sentencia de 1 de Julio de 2002, sobre el tratamiento de datos de clientes en casinos de juego; la sentencia de 23 de septiembre de 2002, sobre la utilización de datos de las listas del censo electoral; la sentencia de 22 de noviembre de 2002, sobre la falta de identidad de hechos, fundamentos y pretensiones para que proceda casar la sentencia impugnada; la sentencia de 23 de abril de 2003, sobre el tratamiento de datos procedentes de fuentes no accesibles al público; la sentencia de 18 de septiembre 2003, sobre que no existe contradicción entre la doctrina de la sentencia recurrida y la que se invoca como de contradicción, o la sentencia de 31de marzo de 2004, de la Sala de lo Militar, sobre que el Derecho Fundamental a la Protección de Datos de Carácter

---

sentencia, aportada por certificación, es errónea, la decisión de la sentencia recurrida, al declarar ajustado a Derecho el acuerdo sancionador de la Agencia de Protección de Datos por el que se imponía a la recurrente una multa de diez millones una mil pesetas como responsable de una infracción grave tipificada en el artículo 43.3 f) de la Ley Orgánica 5/1992, es acertada y correcta, de manera que se debe declarar que no ha lugar al recurso de casación interpuesto para la unificación de doctrina".

[221] Esta sentencia establece en su F.Jº. 4º que: (...) "mientras que en la sentencia recurrida, a pesar de haberse planteado por la demandante tal cuestión, se omite cualquier referencia a ella para limitarse a declarar que "parece olvidar la actora que la conducta sancionada no es el registro del dato, sino mantener en el fichero de que es titular, en la fecha de la reclamación y de la inspección, el registro de una deuda saldada en 1995 (artículo 43.3 f) de la LORTAD)", terminando con la declaración de ser ajustado a derecho el acuerdo recurrido en cuanto sancionó a la entidad demandante por la infracción tipificada en este último precepto".

[222] En esta otra sentencia, se desestima el recurso aludiendo a la" falta del requisito de identidad de fundamentos en la sentencia recurrida, por lo que se hacía necesario desestimar el recurso interpuesto: En el caso presente la recurrente simplemente alega que distintas sentencias anteriores de la Sala de la Jurisdicción de la Audiencia Nacional hicieron aplicación de un precepto que no se invocó en su demanda por el recurrente ni se aplicó en el caso de la recurrida, lo que por sí solo habría de dar lugar a la desestimación del recurso puesto que, evidentemente, no concurre el requisito exigible conforme al artículo 96.1 de que el pronunciamiento de la sentencia llegue a resultados diferentes con fundamentos y pretensiones sustancialmente iguales" (F.Jº. 2º).

Personal debe prevalecer sobre el contenido de determinadas órdenes militares.

Como se ha dicho, todas estas resoluciones centran sus fallos en la desestimación del recurso de casación, y no se estudian con mayor detalle en la presente exposición debido a la escueta trascendencia que, en materia de protección de datos de carácter personal, han tenido. Incluso otras sentencias en las que sí se estimaron los recursos interpuestos, como la Sentencia de 29 de Julio de 2000[223], sobre qué es el responsable del fichero, quién está sujeto al régimen sancionador, y no quien le facilita el dato en virtud de un contrato celebrado con aquél, se centran en temas formales más que materiales.

Además de la importantísima aportación jurisprudencial vista, las autoridades de control realizan su propia aportación a la definición de la protección de datos, con su labor interpretativa, porque aún no tratándose de legislación propiamente dicha, han jugado un importante papel en su cometido aclaratorio en la aplicación práctica de las normas, y porque no se puede afirmar que con la LOPD y el Reglamento de Medidas de Seguridad estén cubiertas todas las necesidades de regulación, de forma clara y concisa. Y es que en realidad, ha venido siendo la potestad instructora[224] de la Agencia Española de Protección de Datos la que ha estado resolviendo en gran medida, junto con la labor judicial ya mencionada, los términos "oscuros" y las dudas que en general se han ido dando en su aplicación práctica.

[223] En esta sentencia se señaló que: "Este motivo de impugnación debe ser estimado, pues como declaró recientemente esta Sala y Sección al resolver, en sentencia de trece de abril de dos mil dos, el recurso de casación para unificación de doctrina –3372/2001– el responsable del fichero es quien decide sobre la finalidad, contenido y uso del tratamiento automatizado y no quien le facilita el dato en virtud de un contrato celebrado con aquél, de modo que sólo el responsable del fichero está sujeto al régimen sancionador establecido en la aludida Ley Orgánica, ya que conforme a la letra y el espíritu del artículo 28, no cabe extender a cualquier otra persona, pues, de hacerlo, como la sentencia recurrida, se incurre en una aplicación extensiva o analógica del régimen sancionador, prohibida por el artículo 25.1 de la Constitución y 129.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, con manifiesta conculcación de los principios de legalidad y tipicidad, y por consiguiente la mencionada sentencia debe ser anulada." (F.Jº. 1º).

[224] Artículo 36. c) de la LOPD: "Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley".

A nivel estatal, la Agencia Española de Protección de Datos, tiene entre las funciones públicas de la tarea específica de dictar las instrucciones precisas para adecuar los tratamientos a los principios de reguladores de la LOPD[225], siendo de las primeras más relevantes:

- La Instrucción 1/1995 de 1 de marzo de la APD relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.
- La Instrucción 1/1998, de 19 de enero, de la APD, relativa al ejercicio de los derechos de acceso rectificación y cancelación.
- Instrucción 1/2000, de 1 de diciembre, de la APD, relativa a las normas por las que se rigen los movimientos internacionales de datos.
- Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones.
- Instrucción 1/2006 de 8 de noviembre de 2006, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

A nivel autonómico, existen hoy tres Agencias o autoridades de control, la de Madrid, la de Cataluña, y la del País Vasco, con sus respectivas normas de creación como Autoridades de Control autonómicas[226], y están aún en proyecto otras como la de Galicia o la de Castilla la Mancha.

Estas Autoridades tienen como misión velar por la defensa de la protección de datos de carácter personal en los correspondientes territorios, y por el respeto de la normativa específica del Sector Público, y en

[225] Se puede consultar su contenido en la página web de la Agencia Estatal de Protección de Datos (www.agpd.es) Otras: Instrucción 2/1995, de 4 de mayo, de la AEPD, sobre garantía de los datos personales recabados en la contratación de seguro de vida de forma conjunta con un préstamo hipotecario o personal, Instrucción 1/1996, de 1 de marzo, de la AEPD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios, Instrucción 2/1996, de 1 de marzo, de la AEPD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.

[226] Ley 8/2001 (CAM), de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid; Ley 5/2002 (Comunidad Autónoma de Cataluña), de 19 de abril, de la Agencia Catalana de Protección de Datos; Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

cumplimiento de lo dictaminado por la STC 292/2000, de 30 de noviembre, en cuanto a que la actividad pública de protección de datos debe materializar la distribución de competencial entre Estado y CCAA, son los organismos encargados de velar por la correcta aplicación de las disposiciones de protección de datos en su territorio, específicamente lo que atañe a los ficheros del sector público, en la Comunidad Autónoma que corresponda[227] y, actuando con plena independencia de la Administración del éstas.

De su ámbito competencial material, los sectores más relevantes en que participan como garantes de la protección de los datos de los administrados, son tal vez, el sector sanitario, el sector educación pública, los ficheros de la administración local, los ficheros de Colegios Profesionales y Cámaras de Comercio. La aplicación de la normativa específica, para las entidades de derecho público, ha supuesto una tarea complementaria de interpretación de las agencias autonómicas, pues desde las normas de creación de los ficheros de estas entidades, las normas sancionadoras, o incluso los principios ordenadores de la LOPD, son expuestos con matices y excepciones para este ámbito, diferentes al del sector privado[228]. Por ejemplo, el principio de calidad de los datos, que obliga a la cancelación de los datos irrelevantes o que han dejado de ser útiles, en el caso de la Administración Pública, jueces y Tribunales, podrán conservase bloqueados por una cuestión de interés público. El principio general del consentimiento, cede cuando los datos se recogen para el ejercicio propio de las funciones de las administraciones, o de competencias homogéneas (que no versen sobre materias distintas), o para el tratamiento de los datos con fines históricos, estadísticos o científicos. Además, podrán ser objeto de comunicación los datos elaborados u obtenidos por una Administración Pública, con destino a otra. Los derechos de acceso, rectificación y oposición, también están matizados, en el caso de los ficheros de las Fuerzas y Cuerpos de Seguridad

[227] Artículo 41.1. "Órganos correspondientes de las Comunidades Autónomas. Las funciones de la Agencia Española de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j, k y l, y en los apartados f y g en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido".

[228] "La contribución de las Agencias Autonómicas al derecho fundamental a la protección de datos". *XVII Encuentros sobre Informática y Derecho*. 2002 – 2003. Universidad Pontificia de Comillas. Ed. Aranzadi. Madrid, 2003. p. 33.

del Estado, o los que afecten a la Defensa Nacional, por su relevancia en materia de seguridad estatal (artículo 22 y 24 LOPD).

En todo caso, las relaciones entre la Agencia de Protección de Datos del Estado y las Agencias de Protección de Protección de Datos de las Comunidades Autónomas, mantienen un funcionamiento integrado basado en los principios de cooperación y coordinación, para garantizar la existencia de un único derecho a la protección de datos en todo el territorio nacional, independientemente del lugar de residencia del afectado.

Importante es también citar al menos la labor del Consejo Consultivo de Protección de Datos[229], el órgano colegiado que asesora directamente al Director de la Agencia Española de Protección de Datos, emitiendo informes sobre las cuestiones que éste le someta, y formulando las propuestas que considere oportunas en temas de su competencia.

2.4.- Legislación y contribución jurisprudencial de la Unión Europea y Estados miembros.

Si bien es cierto que el punto de partida de la actual conceptuación del derecho a la protección de datos en Europa, debe considerarse sin dudas en la ya citada Sentencia del Tribunal Constitucional Alemán de 1983 sobre el censo poblacional, por referirse al contenido del "derecho fundamental a la

[229] Artículo 38 LOPD. Consejo Consultivo. "El Director de la Agencia Española de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros: Un Diputado, propuesto por el Congreso de los Diputados. Un Senador, propuesto por el Senado. Un representante de la Administración Central, designado por el Gobierno. Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias. Un miembro de la Real Academia de la Historia, propuesto por la misma. Un experto en la materia, propuesto por el Consejo Superior de Universidades. Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente. Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma. Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente. El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan".

autodeterminación informativa", en realidad, las preocupaciones que llevarían a incorporar referencias legales a la protección de datos en los diferentes Estados miembros, comenzaron a surgir desde finales de los años 60 en con motivo del nacimiento de la Unión Europea.

En 1967 se constituyó Comisión Consultiva en Europa, que se dedicaría a estudiar la potencial agresividad de la tecnología sobre los derechos de los individuos, y elaboraría el dictamen que informaría la Resolución 509 de la Asamblea del Consejo de Europa sobre los derechos humanos y los nuevos logros científicos, de 1968, que se centraba principalmente en el derecho a no sufrir injerencias en la vida privada, que ya se había recogido en el artículo 12 de la Declaración Universal de Derechos Humanos, o en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966.

Casi diez años más tarde, el Consejo de Europa publicó dos resoluciones para la ordenación del sector público en relación con los tratamientos electrónicos de bancos de datos, una en 1973 y otra en 1974[230]. En su contenido se plasman una serie de exigencias de exactitud en la información que se daba a las personas afectadas por los tratamientos de datos personales, sobre la libre circulación de datos, la accesibilidad a los registros de sus datos, el deber de secreto de quienes trataban los datos de carácter personal, la seguridad necesaria para una eficaz conservación y procesamiento de los datos y, la garantía de disociación para aquellos tratamientos de datos en que los que no fuera necesario identificar a su titular.[231]

El Parlamento Europeo, con fecha 8 de mayo de 1979 aprobó la Resolución sobre la tutela de los derechos del individuo frente al creciente

---

[230] Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector. Se puede ver su texto en http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20%2873%29%2022.asp#TopOfPage
Resolution (74) 29 on the protection of individuals vis-à-vis electronic data banks in the public sector. http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20%2874%29%2029.asp#TopOfPage

[231] DAVARA RODRÍGUEZ, M.A., *La protección de datos en Europa*. Grupo Asnef Equifax. Madrid, 1998. p. 30.

progreso técnico en el sector de la informática, y, el 28 de Enero de 1981 fue aprobado por el Consejo de Europa el Convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, es el Convenio Nº 108. Fue ratificado por España en 1984, publicándose en el BOE el 15 de noviembre de 1985 y, de conformidad con el artículo 96 de nuestra Constitución, este paso significó su incorporación al derecho interno. El Convenio reconocía la posibilidad de que cada Estado parte pudiera, en su legislación interna, establecer excepciones y restricciones a los principios y derechos señalados. Señalaba que podría ser así, en su artículo 9.2, siempre y cuando tales excepciones constituyesen "una medida necesaria en una sociedad democrática, y marcaba cuáles pueden ser éstos supuestos: para la protección de la seguridad del Estado, y para la protección de la persona concernida y de los derechos y libertades de otras personas". En cualquier caso, se trata de un texto que no es de aplicación directa, por tanto, debían ser los propios Estados los que decidieran establecer los instrumentos necesarios para hacer efectivo su contenido.

Tras la entrada en vigor de este Convenio, el Consejo de Europa comenzó a dictar Recomendaciones[232] muy significativas en éste ámbito, y que son de referencia obligada para entender el marco legislativo actual de nuestro país. Entre otras, cabe destacar por su relevancia sectorial, las siguientes:

- Recomendación R (81) 1 del Comité de Ministros a los Estados miembros relativa a la reglamentación aplicable a los bancos de datos médicos automatizados.[233]
- Recomendación R (85) 20 del Comité de Ministros a los Estados miembros relativa a la protección de los datos de carácter personal utilizados con fines de marketing directo.

[232] Disponible en: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection

[233] Actualizada años después por la Recomendación R (97) 5 del Comité de Ministros a los Estados miembros relativa a la protección de datos médicos.

- Recomendación R (87) 15 del Comité de Ministros a los Estados miembros dirigida a regular la utilización de datos de carácter personal en el sector de la policía.

- Recomendación R (92) 1 del Comité de Ministros a los Estados miembros sobre la utilización de los análisis de ácido desoxirribonucleico (ADN) dentro del marco del sistema de justicia penal.

- Recomendación R (95) 4 del Comité de Ministros a los Estados miembros sobre la protección de los datos de carácter personal en el ámbito de telecomunicación, especialmente en lo que se refiere a los servicios telefónicos.

- Recomendación R (97) 18 relativa a la protección de datos personales recogidos y tratados con fines estadísticos.

- Recomendación R (99) 5 relativa a la protección de la intimidad en Internet.

- Recomendación R (02) 9 relativa a la protección de datos personales recogidos y tratados con fines relacionados con el seguro.

Paralela a esta labor legislativa, es importante citar también la labor de la Organización para la Cooperación y Desarrollo de Europa (OCDE), pues mostró igualmente su preocupación en materia de protección de datos personales dictando la Recomendación del Consejo Relativa a las directrices que rigen en la protección de la intimidad y de la circulación transfronteriza de datos personales[234]. En el prólogo se dice que las "Directrices, en forma de Recomendación del Consejo de la OCDE, fueron elaboradas por un grupo de expertos gubernamentales" (...) La Recomendación fue adoptada y entró en vigor el 23 de septiembre de 1980. Unidas a la Recomendación, aparecen las Directrices relativas a la protección de la intimidad y de la circulación de datos personales y, el artículo 6 pone de manifiesto la fuerza vinculante que debería tener todo su contenido para los Estados destinatarios: "Estas Directrices deberían considerarse como criterios mínimos susceptibles de suplementarse con medidas adicionales para la protección de la intimidad y las libertades individuales".

[234] Recomendación del Consejo en relación con las Directrices que rigen la Protección de la Intimidad y Tránsitos Transfronterizos de Datos Personales del 23 de Septiembre de 1980.

Merece la pena señalar en este punto que, en la misma línea, otro organismo de carácter internacional como es la Asamblea de Naciones Unidas adoptaba sus propias directrices de protección de datos: la Resolución 45/95 de la Asamblea General, el 14 de diciembre de 1990 y, establecen "los procedimientos para llevar a la práctica las normas relativas a los archivos de datos personales informatizados se dejan a la iniciativa de cada Estado, con sujeción a las siguientes orientaciones, y señala dos puntos concretos a desarrollar: a) Garantías mínimas que deben prever las legislaciones nacionales, y b) Aplicación de las directrices a archivos de datos personales mantenidos por organizaciones internacionales gubernamentales". Concluye este texto con una "Cláusula humanitaria" que merece la pena citar textualmente, por su carácter restrictivo de los valores fundamentales genéricos, ante la dignidad humana: "puede preverse específicamente una excepción a estos principios cuando la finalidad del archivo sea la protección de los derechos humanos y las libertades fundamentales de la persona afectada, o la ayuda humanitaria".

Actualmente las Directivas del Parlamento Europeo y del Consejo se ocupan de homologar la situación jurídica de los diferentes territorios que conforman el espacio europeo, y la más importante, es sin duda, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, es la norma más importante[235] dictada en esta materia, porque fija los mínimos que deben ser transpuestos en las normativas estatales del territorio UE y, además, porque actúa como norma supletoria. Además, fue la norma que

[235] Otras: Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso), Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización), Directiva 2002/21/CE, del parlamento Europeo y del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas., Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal), Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas), Directiva 2004/82/CE, del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

reclamó de los Estados miembros, un actualizado desarrollo legislativo acorde con su mandato y con el Convenio 108 del Consejo de Europa de 1981 (ratificado por España en 1984) y, en España, se encargó de ello la Ley Orgánica 15/1999 de protección de datos de carácter personal, traduciendo el sistema europeo a nuestro derecho interno. El artículo 29 de esta Directiva, crea además el "Artículo 29 Working Party", un grupo de trabajo especializado en el estudio de la protección de las personas en lo que respecta al tratamiento de sus datos de carácter personal.

En el año 2000, se proclamó la Carta de los Derechos Fundamentales de la Unión Europea, firmada por los Presidentes del Parlamento, del Consejo y, de la Comisión europeas, con ocasión del Consejo Europeo de Niza. Este texto, no otorga derechos nuevos a sus destinatarios, pero sí tiene el mérito tener en cuenta nuevas inquietudes y necesidades de garantía que han surgido con el progreso de las sociedades, tiene en cuenta la "Sociedad de la Información", y de consolida definitivamente la diferencia entre el derecho a la intimidad[236] y el derecho a la protección de datos, en el artículo 8, señalando específicamente que:

> "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

Este artículo está redactado sobre el espíritu del artículo 286 del Tratado constitutivo de la Comunidad Europea, de la Directiva 95/46/CE y, del el artículo 8 del Convenio del Consejo de Europa para la protección de las

[236] Artículo 7. Respeto a la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 (Convenio Nº 108). Todas estas normas fueron también la base para la actividad del Grupo de Trabajo[237] del Artículo 29 de la Directiva 95/46/CE. Se trata del órgano asesor de la UE sobre protección de los datos y la vida privada. Es independiente y, sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14. 3 de la Directiva 97/66/CE[238].

El artículo 30 señala que el "Grupo tendrá por cometido:

> a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;
>
> b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;
>
> c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así

[237] Algunos de sus trabajos, son: el Dictamen 1/98 sobre Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS), el Dictamen 1/99 relativo al nivel de protección de datos en Estados Unidos y a los debates en curso entre la Comisión Europea y el Gobierno de Estados Unidos, la Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware, la Recomendación 2/99 sobre La protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, el Dictamen 2/99, relativo a la idoneidad de los "Principios internacionales de puerto seguro", la Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, el Dictamen 4/99 Inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales, el Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico, el Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones, el Dictamen 7/2000 sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, el Dictamen 4/2001 acerca del proyecto de convenio del Consejo de Europa sobre el ciberdelito, el Dictamen 10/2001 relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo, el Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, el Dictamen 1/2003 sobre el almacenamiento de los datos sobre tráfico a efectos de facturación, etc.

[238] Artículo 14.3 de la Directiva 97/66/CE, establece que: "El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido con arreglo al artículo 29 de la Directiva 95/46/CE ejercerá las funciones especificadas en el artículo 30 de la citada Directiva también por lo que se refiere a la protección de los derechos y libertades fundamentales y de los intereses legítimos en el sector de las telecomunicaciones, que son objeto de la presente Directiva".

como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;

e) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria"[239].

De este cometido se puede deducir que sus trabajos (informes, recomendaciones, dictámenes), aun no siendo vinculantes, aportan a la interpretación de la normativa en materia de protección de datos una dosis de actualidad y congruencia práctica fundamental para determinar la calificación jurídica de los hechos que se van dando en la realidad del entorno europeo en esta materia.

Otras Directivas europeas que han ido orientando la evolución de la garantía de la protección de la información personal, son la Directiva 2002/58/CE, de 12 de julio, del Parlamento Europeo y del Consejo, sobre tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas y, Directiva 2006/24/CE, de 15 de marzo, del Parlamento Europeo y del Consejo, sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y modifica Directiva 2002/58/CE, de 12 julio de 2002[240].

---

[239] Continúa:
"2. Si el Grupo comprobare la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión.
3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.
4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión y al Comité contemplado en el artículo 31.
5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado.
6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado".

[240] Otras: Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores; Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE; Directiva 2004/82/CE, del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas; Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal

Asimismo, también los Reglamentos del Parlamento Europeo y del Consejo han contribuido a dotar de un contenido cada vez más preciso y ordenado de esta materia, tales como el Reglamento (CE) nº 45/2001 de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[241], o el Reglamento (CE) nº 831/2002 de la Comisión Europea, de 17 de mayo de 2002, por el que se aplica el Reglamento (CE) no 322/97 del Consejo sobre la estadística comunitaria en lo relativo al acceso con fines científicos a datos confidenciales. Las Decisiones de la Comisión Europea, relativas a la protección adecuada de los datos personales en diferentes países (con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo)[242], o las Decisiones relativas a la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren a terceros países[243], completan aquellas otras previsiones.

De obligada referencia es además el proyecto de Tratado por el que se instituye una Constitución para Europa, en la versión entregada al Presidente del Consejo Europeo en Roma, el 18 de julio de 2003, que recoge expresamente el derecho a la Protección de Datos Personales. Especialmente interesante y notorio es el hecho de que expresamente recoja dos artículos sobre el Derecho Fundamental a la Protección de Datos de Carácter Personal. El primero, enmarcado en "La definición de los objetivos de la Unión" (I-

y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).; Directiva 2002/21/CE, del parlamento Europeo y del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas; Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización); Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso); Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico); Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

[241] También: el Reglamento (CE) nº 2725/2000 del Consejo, de 11 de diciembre de 2000, relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín. DOCE L 316/1 de 15 de septiembre de 2000.

[242] Estados Unidos ("puerto seguro"), Hungría y Suiza, del año 2000; Canadá, de 2001; Argentina, Isla de Man y Guernsey, del año 2003; Jersey, de 2008; Islas Feroe y Andorra, de 2010.

[243] Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a "Cláusulas contractuales tipo para la transferencia de datos personales a un tercer país" previstas en la Directiva 95/46/CE (y posteriores modificaciones, aprobadas en 2002, 2004, 2005 y 2010, esta última es la Decisión de la Comisión (2010/87/UE), de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo).

51)[244]. El segundo, enmarcado en la "Carta de los Derechos Fundamentales de la Unión" (II-68)[245]. Como se ha señalado, este derecho estaba incluido en la Carta de Derechos Fundamentales del año 2000 (Niza), como artículo de relación directa con la vida democrática.

Por otra parte, con el "Tratado Lisboa", firmado en Lisboa el 13 de diciembre de 2007, los Jefes de Estado o de Gobierno tuvieron presentes los cambios políticos, económicos y sociales que se estaban produciendo y, con ello, la necesidad de responder a las expectativas de los ciudadanos europeos sobre qué puede o no puede hacer la UE, y qué medios puede utilizar. Modifica la estructura de las instituciones europeas y sus métodos de trabajo, para dar un mejor servicio a la democracia y a los valores fundamentales de la Unión. El texto resultante de las negociaciones entre los Estados miembros reunidos en la Conferencia Intergubernamental, en la que participaron también la Comisión y el Parlamento Europeo, fue ratificado por los 27 Estados miembros de la UE, entrando en vigor el 1 de diciembre de 2009, según lo dispuesto en su artículo 6.

Este Tratado modifica los dos principales Tratados de la UE (pero no los sustituye), el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea (pasando este último a llamarse Tratado de Funcionamiento de la Unión Europea), para ofrecer un marco regulador que procure, una Europa más democrática, más transparente y, más eficaz, que potencie los valores de la Unión de derechos y valores, libertad, solidaridad y seguridad[246].

En la materia que nos ocupa, este acuerdo, viene a dotar a la UE de medios suplementarios para afrontar el reto de garantizar el pleno respeto del derecho fundamental a la protección de los datos personales, tanto en la UE como fuera de ésta. Así, la Carta de los Derechos Fundamentales de la

[244] "Artículo I-53. Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. La ley o ley marco europea establecerá las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. 3. El respeto de dichas normas estará sometido al control de autoridades independientes".

[245] Artículo II-68. Ibídem.

[246] Véase: "El Tratado en pocas palabras": http://europa.eu/lisbon_treaty/glance/index_es.htm

UE, en cuyo artículo 8 se reconoce el derecho autónomo a la protección de los datos personales, es en adelante jurídicamente vinculante, y se crea una nueva base jurídica[247], que permite la elaboración de una normativa global y coherente en materia de protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos, para la UE. Esta nueva base jurídica autoriza, en particular, a la Unión a regular la protección de datos por medio de un único instrumento jurídico, en particular, en los ámbitos de la cooperación policial y la cooperación judicial en materia penal. La Política Exterior y de Seguridad Común sólo está cubierta parcialmente por el artículo 16 TFUE, dado que una decisión del Consejo, con una base jurídica distinta, debe establecer normas específicas aplicables a los tratamientos de datos efectuados por los Estados miembros en este ámbito[248].

El Tratado de la Unión Europea recogía el compromiso de la colaboración policial entre los Estados miembros, en el que se llamaba III Pilar de la Unión Europea, y aunque no existen reglas armonizadas en el nivel europeo, existen la Decisión Marco 2006/960/JAI del Consejo de 18 de diciembre de 2006 sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, y la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, que se verán en el apartado correspondiente a la seguridad de los tratamientos de datos por las autoridades policiales.

En la actualidad, las preocupaciones de la Comisión Europea, sobre protección de los datos personales en el territorio europeo, han sido puestas de manifiesto al Parlamento Europeo a través de la Comunicación de fecha 4 de Noviembre de 2010[249]. En este informe, reconoce que "al igual que la tecnología, la forma en que nuestros datos personales se utilizan y

[247] Véase el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE).
[248] Véase el artículo 16, apartado 2, último párrafo, del TFUE y el artículo 39 del Tratado de la Unión Europea (TUE).
[249] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Un enfoque global de la protección de los datos personales en la Unión Europea*. COM(2010) 609 final. Bruselas, 4.11.2010.

comparten en nuestra sociedad está en evolución constante. El reto que esto plantea a los legisladores es el de establecer un marco legislativo que resista al tiempo. Al final del proceso de reforma, las normas europeas de protección de datos deberían seguir asegurando un elevado nivel de protección y garantizando la seguridad jurídica a las personas, a las Administraciones públicas y a las empresas en el mercado interior, durante varias generaciones. Independientemente de la complejidad de la situación o de la sofisticación de la tecnología, es esencial que las normas que deben aplicar las autoridades nacionales y que deben cumplir las empresas y los responsables del desarrollo de tecnologías, estén claramente definidas. Del mismo modo, las personas deben tener claros los derechos de que gozan*"*[250]*.* Asimismo, manifiesta su intención de fomentar las iniciativas en materia de autorregulación y examinar la posibilidad de instaurar regímenes europeos de certificación; de revisar las normas de protección de datos en los ámbitos de la cooperación policial y judicial en materia penal; de examinar "los medios para mejorar y racionalizar los procedimientos actuales de transferencia internacional de datos, incluidos los instrumentos jurídicamente vinculantes y las "normas vinculantes para las empresas", con el fin de lograr un enfoque de la UE más uniforme y más coherente respecto a los terceros países y las organizaciones internacionales; clarificar su procedimiento de evaluación del carácter adecuado del nivel de protección garantizado en un tercer país o una organización internacional y precisar los criterios y condiciones aplicables, y definir los elementos esenciales en materia de protección de datos que deberían utilizarse en todos los tipos de acuerdos internacionales celebrados por la UE*"*[251].

Respecto de los derechos de los ciudadanos, aún hoy se continúa planteando la Comisión estudiar la manera de garantizar una aplicación coherente de las normas de protección de datos, habida cuenta de las repercusiones de las nuevas tecnologías en los derechos y libertades de las personas, y habida cuenta del objetivo consistente en garantizar la libre circulación de datos personales en el mercado interior, para tratar de

[250] Ibídem. Apdo. 2.4. La dimensión mundial de la protección de datos. Clarificar y simplificar las normas aplicables a las transferencias internacionales de Datos. p. 18.
[251] Ibídem. Apdo. 3 Conclusiones: Perspectiva Futura. p. 3.

introducir, en el marco jurídico, "un principio general que imponga el tratamiento transparente de los datos personales; introducir obligaciones específicas para los responsables del tratamiento relativas al tipo de información que debe comunicarse y a las modalidades de su comunicación, incluso por lo que se refiere a los niños; elaborar uno o más modelos normalizados europeos ("declaraciones de confidencialidad") que deberán utilizar los responsables del tratamiento"[252]. Otras intenciones que se manifiestan en este informe, son:

- mejorar las condiciones de un verdadero ejercicio de los derechos de acceso, rectificación, supresión y bloqueo (por ejemplo, fijando plazos de respuesta a las solicitudes de las personas en cuestión, autorizando el ejercicio de estos derechos por vía electrónica o instaurando la gratuidad como principio del ejercicio del derecho de acceso);

- clarificar el llamado "derecho a ser olvidado", es decir, el derecho de las personas a que sus datos no se traten y se supriman cuando dejan de ser necesarios con fines legítimos. Se trata, por ejemplo, del caso en que la persona retira su consentimiento al tratamiento de datos, o del caso en que haya expirado el plazo de conservación de los datos;

- completar el abanico de los derechos de los interesados garantizando la "portabilidad de los datos", es decir, confiriendo a los individuos el derecho explícito a retirar sus datos (por ejemplo, fotografías o listas de amigos) de una aplicación o de un servicio, de modo que los datos retirados puedan transferirse a otra aplicación u otro servicio, siempre que ello sea técnicamente posible, sin que los responsables del tratamiento lo obstaculicen.

- determinar si otras categorías de datos deberían considerarse "sensibles", por ejemplo, los datos genéticos;

[252] Ibídem. Apdo. 2.1. Reforzar los derechos de las personas. Aumentar la transparencia para los interesados. p. 7.

- precisar aún más y armonizar las condiciones que deben cumplirse para realizar el tratamiento de determinadas categorías de datos sensibles.

Explica esta comunicación que la Directiva relativa a la protección de datos de 1995, quince años más tarde, el doble objetivo que marcaba, es decir, la protección de los derechos y libertades fundamentales de las personas, del derecho fundamental a la protección de datos, y, la realización del mercado interior, caso, la libre circulación de datos personales, sigue teniendo vigencia y los principios consagrados en dicho texto. Sin embargo, reconoce que la rapidez de la evolución tecnológica y la globalización han modificado profundamente nuestro medio[253] y han lanzado nuevos retos en materia de protección de los datos personales. Estos retos pasan por intentar una mayor armonización de las normas de protección de datos en la UE, una mejora de los derechos de los interesados, y una mejora de las garantías que los protejan.

La Comisión Europea trabaja activamente en la actualización de normas, y lo hace consciente de que La Directiva 95/46/EC tiene más de quince años, y eso en Internet es demasiado tiempo para un acervo regulador tan importante. Con el firme propósito de armonizar las normas de los Estados miembros, y de integrarlas en el contexto del presente, se ha tomado la decisión de aprobar un Reglamento que establezca un marco general de la UE para la protección de datos, y una Directiva, sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y en relación con las actividades judiciales correspondientes[254].

En general, según una nota de prensa emitida por la Comisión Europea, de 25 de Enero de 2012, las propuestas de modernización de los

[253] Ibídem. (…) "los métodos de recogida de los datos personales son cada vez más complicados y se detectan con más dificultad". Apdo. 1. Nuevos retos en materia de protección de datos. p. 2.
[254] "La protección de los datos personales es un derecho fundamental de todos los europeos, quienes, no obstante, a veces sienten que pierden el control sobre sus datos personales. Mis propuestas contribuirán a infundir confianza en los servicios en línea dado que los ciudadanos estarán mejor informados de sus derechos y tendrán un mayor control sobre la información que les atañe. La reforma conseguirá todos estos objetivos al tiempo que facilitará el funcionamiento de las empresas y les permitirá ahorrar costes. La existencia de un marco legal sólido, claro y uniforme a escala de la UE permitirá liberar el potencial del Mercado Único Digital y fomentar el crecimiento económico, la innovación y la creación de empleo". Viviane Reding, Comisaria de Justicia de la UE y Vicepresidenta de la Comisión. Comunicado de Prensa de la Comisión Europea. 25 de Enero de 2012.

principios sobre protección de datos, constan de una Comunicación en la que se exponen los objetivos de la Comisión y dos propuestas legislativas: un Reglamento[255] que establece un marco general de la UE para la protección de datos y una Directiva[256] sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y en relación con las actividades judiciales correspondientes.

Según la Comisión, el 4 de noviembre de 2010, se fijó "una estrategia para reforzar las normas de protección de datos de la UE (IP/10/1462 y MEMO/10/542). Sus objetivos eran proteger los datos personales en todos los ámbitos de actuación, incluido el orden público, reduciendo al mismo tiempo los trámites engorrosos para las empresas y garantizando la libre circulación de datos dentro de la UE. La Comisión solicitó reacciones a sus ideas y llevó a cabo una consulta pública por separado para revisar la Directiva sobre protección de datos (95/46/CE)", y hoy, es claro que hace falta una actualización normativa que tenga en cuenta:

[255] Necesario en un contexto legal desactualizado, del que, según la Exposición de Motivos: "La piedra angular de la legislación vigente de la UE en materia de protección de datos, la Directiva 95/46/CE3, fue adoptada en 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros. Se complementó mediante la Decisión Marco 2008/977/JAI, en su calidad de instrumento general a escala de la Unión para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. La rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales. Se ha incrementado enormemente la magnitud del intercambio y la recogida de datos. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social. (...) El artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE), introducido por el Tratado de Lisboa, establece el principio según el cual toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Además, con el artículo 16, apartado 2, del TFUE, el Tratado de Lisboa introdujo una base jurídica específica para la adopción de normas relativas a la protección de datos de carácter personal. El artículo 8 de la Carta de los Derechos Fundamentales de la UE consagra como derecho fundamental la protección de los datos de carácter personal. Asimismo, se considera que un Reglamento es el instrumento jurídico más apropiado para definir el marco de la protección de datos personales en la Unión. La aplicabilidad directa de un reglamento, de conformidad con el artículo 288 del TFUE, reducirá la fragmentación jurídica y ofrecerá una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento del mercado interior". Disponible la propuesta de Reglamento (15.02.2012) en: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf

[256] La propuesta de Directiva se basa en el artículo 16, apartado 2, del TFUE, que es una nueva base jurídica específica introducida por el Tratado de Lisboa, y tiene por objeto tiene por objeto "garantizar un nivel uniforme y elevado de protección de los datos en este ámbito, reforzando así la confianza mutua entre las autoridades policiales y judiciales de los distintos Estados miembros y facilitando la libre circulación de datos y la cooperación entre las autoridades policiales y judiciales". Disponible a 15.02.2012 en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:ES:PDF

- "un conjunto único de normas sobre protección de datos válido en toda la UE y se eliminarán requisitos administrativos innecesarios como los requisitos de notificación para las empresas",
- "intensificar la responsabilidad y la obligación de rendir cuentas de todos aquellos que procesen datos personales",
- que las empresas y organizaciones tengan la obligación de "notificar a la autoridad nacional de control toda violación de datos grave lo antes posible" (siempre que sea posible en un plazo de 24 horas).
- que las organizaciones tengan "como interlocutora única a una autoridad nacional de protección de datos en el país de la UE donde tengan su sede, y los ciudadanos puedan dirigirse a la autoridad de protección de datos de su país, incluso cuando sus datos sean tratados por una empresa ubicada fuera de la UE".
- que siempre "que el tratamiento de los datos exija el consentimiento del interesado, deberá dejarse claro que dicho consentimiento debe obtenerse explícitamente y no presuponerse".
- que los ciudadanos tengan un "acceso más fácil a sus propios datos y deberán poder transferir sus datos personales de un proveedor de servicios a otro con mayor facilidad" (derecho a la "portabilidad de los datos").
- que el "derecho al olvido" ayudará a los ciudadanos a "gestionar mejor los riesgos inherentes a la protección de los datos en línea: los usuarios podrán borrar sus datos cuando no existan razones legítimas para conservarlos".
- aplicar las "normas de la UE a toda empresa activa en el mercado de la UE que ofrezca sus servicios a ciudadanos de la UE y procese datos personales en terceros países".

Según la Exposición de Motivos de la propuesta de Directiva, aunque de que el Tratado de Lisboa (artículo 16, apartado 2, del TFUE) introduce una base jurídica específica para la adopción de normas relativas a la protección de los datos personales, que también se aplica a la cooperación judicial en materia penal y la cooperación policial, y debido a la naturaleza específica del ámbito de la cooperación policial y judicial en materia penal, "podrían requerirse normas específicas para la protección de datos de carácter

personal y la libre circulación de dichos datos" en este ámbito. Por otra parte, la Decisión Marco 2008/977/JAI[257] no es suficiente: "tiene un ámbito de aplicación limitado, ya que solo se aplica al tratamiento transfronterizo de datos y no a las actividades de tratamiento por parte de las autoridades policiales y judiciales a nivel puramente nacional. Ello puede crear dificultades a las autoridades policiales y otras autoridades competentes en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial. No son siempre capaces de distinguir fácilmente entre el tratamiento meramente nacional y el transfronterizo no de prever si determinados datos personales pueden convertirse en objeto de un intercambio transfronterizo en una fase posterior (véase la sección 2). Además, por su naturaleza y contenido, la Decisión Marco deja un amplio margen de maniobra a los Estados miembros para transponer sus disposiciones de Derecho interno. Por otra parte, no contiene ningún mecanismo o grupo consultivo similar al Grupo del artículo 29 que sustente una interpretación común de sus disposiciones, ni establece competencias de ejecución de la Comisión a fin de garantizar un enfoque común en su aplicación".

Además, la nueva Directiva aplicará ciertos principios y normas generales de protección de datos a la cooperación policial y judicial en materia penal, que se aplicarán a las transmisiones de datos nacionales e internacionales. En este aspecto concreto, la Comunicación[258] destaca que es preciso reforzar el Tratado de Lisboa, reduciendo las diferencias legislativas entre los Estados Miembros, mejorando el flujo de información entre éstos, y reforzando la cooperación en la lucha contra el crimen en Europa. Se trata de garantizar un alto nivel de protección de los datos personales y, a su vez, facilitar los intercambios de información entre las autoridades policiales y judiciales, y para ello se plantean reformas:

[257] Decisión Marco 2008/977/JAI, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. DO L 350 de 30.12.2008.

[258] Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité Regional. "Salvaguardando la privacidad en un mundo conectado. Un marco de trabajo en materia de protección de datos para el siglo XXI". COM. (2012) 9/3. pp. 9 y 10.

- aplicando los principios generales de protección de datos adoptados en el Tratado de Lisboa, de forma que se tenga en cuenta la especialidad de este ámbito de cooperación.
- armonizar mínimamente los criterios, condiciones y límites del tratamiento de datos personales, y en concreto, el derecho de los ciudadanos a ser informados cuando las autoridades policiales y judiciales tratan o acceden a sus datos.
- diferenciar categorías de datos personales para los que pueden variar las garantías legales aplicables a su protección, teniendo en cuenta su especial naturaleza.

Estas propuestas están ahora en fase de discusión ante el Parlamento Europeo y los Estados miembros de la UE (a través del Consejo de Ministros), y no entrarán en vigor hasta dos años después de su adopción.

En el contexto de la Unión Europea, existe también una contribución jurisprudencial[259] muy relevante en materia de protección de datos, que debe ser analizada.

El Tribunal de Justicia de las Comunidades Europeas (TJCE) como el máximo intérprete del Derecho de la UE, garantiza que se aplique de la misma forma en todos los países miembros, orientando sobre cómo debe ser integrada la normativa comunitaria en los ordenamientos internos de los Estados Miembros, y en materia de protección de datos, también ha desarrollado un importantísimo papel, especialmente, a partir del año 2000, esclareciendo especialmente la interpretación que debe darse al artículo 8 del Convenio 108, a la Directiva 95/46/CE y, a la Carta de Derechos Fundamentales de la Unión Europea (2000).

PIÑAR MAÑAS explica que el TJCE ha abordado esta cuestión, considerando que estamos ante un derecho al respeto a la vida privada, que constituye un derecho fundamental protegido por el ordenamiento jurídico comunitario, y cuyo contenido también se ha ido puliendo a través de la

[259] Se puede consultar el texto completo de las sentencias en la página web: www.curia.eu.int

jurisprudencia[260], especialmente, en las Sentencias Lindqvist (2003) y Rundfunk (2003), que luego se analizarán, con consideraciones a elementos concretos del derecho a la protección de datos que merece la pena concretar.

Antes del año 2000, en el año 1994, el TJCE había resuelto el Asunto C-404/92 (de 5 de Octubre de 1994) sobre la obligación de los candidatos a un puesto de trabajo, de someterse a determinadas pruebas médicas, que revelan información de carácter sensible a la entidad contratante. La respuesta de TJCE se basó en el artículo 8 del Convenio 108, en concreto, en el derecho a mantener en secreto el estado de salud[261]: "el derecho al respeto de la vida privada exige respetar la negativa del individuo en toda su extensión"[262] y no puede ser obligado a ser sometido a un reconocimiento médico con el que no se está de acuerdo, aunque, también se reconoce que, ante tal negativa, las Instituciones no están obligadas a correr el riesgo de contratarlo[263].

Más adelante, resolvería este Tribunal en una Sentencia de fecha 14 de Septiembre de 2000, un litigio del Reino Unido ante la High Court of Justice entre The Queen V. Minister of Agriculture, Fisheries & Food[264], sobre la interpretación de los artículos 3, apartado 1, y 9 del Reglamento (CEE) nº 3508/92 del Consejo, de 27 de noviembre de 1992, sobre el sistema integrado de gestión y control de determinados regímenes de ayuda comunitarios para evitar el fraude mediante la imposición de sanciones efectivas en caso de irregularidades o de fraudes[265], analiza la importancia

---

[260] PIÑAR MAÑAS, J.L.,"El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas". *Cuadernos de derecho público*, Nº 19-20. 2003 (Ejemplar dedicado a Protección de datos). p. 56.

[261] Apdo. 17 de la Sentencia.

[262] Apdo. 23 de la Sentencia.

[263] Sentencia TJCE, de 20 de Mayo de 2003 (Rundfunk y otros), Asuntos C-465/00, C-138/01 y, C-139/01), apartado 21.

[264] Judgment of the Court (Fifth Chamber) of 13 November 1990. - The Queen v Minister of Agriculture, Fisheries and Food and Secretary of State for Health, ex parte: Fedesa and others. - Reference for a preliminary ruling: High Court of Justice, Queen's Bench Division - United Kingdom. - Substances having a hormonal action - Validity of Directive 88/146/EEC. - Case C-331/88. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61988CJ0331:EN:HTML

[265] En los apartados número 23, 24 y 25 explica esta sentencia que: "(23) Mediante su primera cuestión el órgano jurisdiccional remitente pide, esencialmente, que se dilucide si los artículos 3, apartado 1, y 9 del Reglamento n. 3508/92, en relación con los principios generales de Derecho comunitario, permiten que las autoridades competentes comuniquen los datos, relativos a los cultivos herbáceos realizados durante los años anteriores y que hayan sido facilitados por o en nombre de un antiguo solicitante de pagos con arreglo al régimen de pagos a tierras de cultivo a un nuevo titular de la explotación que los necesite para poder solicitar tales pagos en relación con las mismas tierras. (24) Del artículo 3, apartado 1, del Reglamento n. 3508/92 se desprende, en primer lugar, que esta norma, al establecer

del tratamiento de datos personales, en relación con el consentimiento del interesado y exige que exista un interés legítimo para poder disponer de datos de carácter personal, excluyendo la voluntad del afectado. Asimismo establece la necesidad de ponderar intereses cuando éstos se manifiesten en conflicto, señalando que: "para responder a la cuestión de si puede facilitarse determinada información contenida en la base de datos, la autoridad competente debe ponderar, por una parte, el interés de la persona que los ha proporcionado y, por otra, el interés de la persona que la necesita para alcanzar un fin legítimo, y que sin embargo, los intereses respectivos de los interesados con respecto a los datos personales deben apreciarse respetando la protección de las libertades y de los derechos fundamentales"[266]. Para, finalmente, sentar en esta cuestión explica que: "procede responder (sobre la cuestión planteada sobre los artículos 3, apartado 1, y 9 del Reglamento n. 3508/92) en relación con los principios generales de Derecho comunitario, permiten que, previa ponderación de los intereses respectivos de las personas afectadas, las autoridades competentes comuniquen los datos relativos a (...) que hayan sido facilitados por o en nombre de un antiguo solicitante de pagos (...) a un nuevo titular de la explotación que los necesite para poder solicitar tales pagos en relación con las mismas tierras y que no pueda obtenerlos de otra manera (apartado número 39)". Esta sentencia resulta de interés por cuanto implica una obligación de especial observancia para los Estados en relación con los derechos fundamentales de sus ciudadanos, en este caso, respecto del concreto derecho a la protección de datos, derecho que considera debe ser protegido en igual medida que otros derechos afines con los que pudiera entrar en conflicto.

Un año más tarde se dictó la Sentencia de 4 de octubre de 2001, respecto de un asunto de la Comisión de las Comunidades Europeas contra el Gran Ducado de Luxemburgo, sobre el incumplimiento de las obligaciones que le incumben en virtud del artículo 32 de la Directiva 95/46/CE, de

---

explícitamente una consulta a la autoridad competente de la base de datos en la que está registrada la información derivada de las solicitudes de ayuda, no descarta que personas distintas de la propia autoridad competente consulten dicha base de datos. (25) Además, el artículo 9 de este mismo Reglamento dispone que los Estados miembros adoptarán las medidas necesarias para garantizar la protección de la información recogida sin, no obstante, hacer precisión alguna".

[266] Apartado 28 de la Sentencia.

adaptación del Derecho Interno a las exigencias comunitarias en materia de protección de datos.

El TJCE reconoce el apartado 94 de la Sentencia Lindqvist (2003) sobre el alcance de la Directiva 95/46, la obligación de transponerla en el plazo establecido y, su aplicabilidad directa en los Estados miembros, aunque señala que esta norma permite a los Estados miembros un margen de apreciación en ciertos aspectos, y establecer regímenes especiales para determinados supuestos, pero, ha de hacerse de conformidad con el principio de proporcionalidad entre la libre circulación de datos personales y la tutela del derecho a la intimidad[267].

Por otra parte se pronuncia sobre el concepto de "protección de datos"[268], explicando que comprende toda información sobre una persona física identificada o identificable, y que incluye "sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones". Y sobre el concepto de tratamiento total o parcialmente automatizado, en particular en Internet, señala "que la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos" es tratamiento y, que "de ello se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales, debe considerarse un tratamiento de esta índole"[269]. Y añade: "la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo u a sus aficiones, constituye un tratamiento total o parcialmente automatizado de datos personales"[270]

También alude a la relación entre este derecho y la libertad de expresión (y otros derechos fundamentales), para concluir que "incumbe a

[267] Apartado 94 de la Sentencia: "nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la Directiva a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello". En el mismo sentido, se pronuncia la Sentencia Rundfunk (2003), en sus apartados 39 y 40.
[268] Apartado 24 de la Sentencia.
[269] Apartado 25 de la Sentencia.
[270] Apartados 26 y 27 de la Sentencia.

las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el justo equilibrio entre los derechos e intereses en juego; incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario[271]" teniendo en cuenta los criterios de la propia Directiva 95/47 al establecer normas que delimiten la protección de datos y la tutela que se le ha de dar.

En el año 2004, otra Sentencia, de 24 de junio, de la Comisión de las Comunidades Europeas contra los Países Bajos, sobre el tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones previsto por los artículos 6 y 9 de la Directiva 97/66/CE, insiste en la condena por haber adaptado de manera incompleta el Derecho Interno de los Países Bajos a dichos preceptos. Siguieron a ésta, las Sentencias, de 14 de septiembre de 2004, de la Comisión de las Comunidades Europeas contra la República de Austria, y de 28 de abril de 2005, de Comisión de las Comunidades Europeas contra la República Italiana.

Otros temas más concretos los han tratado sentencias como la de fecha de 25 de noviembre de 2004, de los Países Bajos, caso KPN Telecom BV y Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), en relación con la puesta a disposición, en beneficio de empresas privadas, de determinada información relativa a los abonados de una operadora de telefonía (KPN), para la elaboración de guías telefónicas por parte de dichas empresas; o la Sentencia de 6 de noviembre de 2003, de Suecia, caso Linqdvist, relativa a la interpretación de la Directiva 95/46, sobre la publicación de datos sensibles sin autorización de su titular en Internet, y también la Sentencia de 20 de mayo de 2003, de Austria, caso Rundfunk Österreichischer, sobre la interpretación de la Directiva 95/46 en materia de divulgación de datos sobre los ingresos de empleados de entidades sujetas al control del Rechnungshof[272].

[271] Apartados 83, 85 y 90 de la Sentencia.
[272] Se citan en último lugar, y cronológicamente en sentido inverso, para dar prioridad al criterio interpretativo de su relevancia respecto a la interpretación de la normativa europea.

La primera de estas resoluciones, señalaba en su apartado número 32 que "no cabe duda de que la protección de los datos personales y la intimidad es un factor primordial que ha de tomarse en consideración cuando se trata de determinar cuáles son los datos que un operador está obligado a poner a disposición de un tercero competidor. En efecto, un criterio amplio, que exija la puesta a disposición indiferenciada de todos los datos de que dispone un operador a excepción, no obstante, de los referentes a los abonados que en modo alguno desean figurar en una lista publicada, no es compatible con la protección tanto de dichos datos como de la intimidad de las personas afectadas"[273]. Delimita claramente el concepto de "información pertinente" y, el principio de calidad, es decir, señala que los datos recabados o tratados no pueden ser excesivos respecto de la finalidad que se pretende.

La segunda resolución (el caso Linqdvist) afirma en su apartado número 27, que la conducta que consiste en hacer referencia, en una página web a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones constituye un "tratamiento total o parcialmente automatizado de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva 95/46. Esta es una de las resoluciones más importantes habidas en materia de protección de datos y la utilización de Internet en la Sociedad de la Información. Establece que el titular de la web, que inserta esos datos poniéndolos a disposición de terceros y, debe estar sujeto a las exigencias de seguridad y confidencialidad que la norma establece, señalando en el apartado número 47 que, únicamente se podrían excepcionar "las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente, no es éste el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de

[273] Y continúa en su apartado número 36 diciendo que "es preciso responder a la primera cuestión que el artículo 6, apartado 3, de la Directiva debe interpretarse en el sentido de que la expresión «información pertinente» se refiere únicamente a los datos relativos a los abonados que no hayan manifestado su oposición a figurar en una lista publicada y que son suficientes para que los usuarios de una guía telefónica puedan identificar a los abonados que buscan. Dichos datos incluyen, en principio, el nombre y la dirección, junto con el código postal, de los abonados, así como el número o números de teléfono que les ha asignado el organismo de que se trate. No obstante, los Estados miembros pueden establecer que se pongan a disposición de los usuarios otros datos cuando, habida cuenta de las condiciones nacionales específicas, parezcan necesarios para la identificación de los abonados".

personas". Este criterio dejó claro por primera vez lo relativo a Internet como medio de comunicación y el alcance de las consecuencias de tratar datos a través de él.

La tercera de las tres sentencias citadas, resolvió el caso Österreichischer, sobre la divulgación de datos sobre los ingresos de empleados de entidades sujetas al control del Rechnungshof.[274] Esta resolución debe su importancia a que trata supuestos de entidades de naturaleza pública. Señaló en sus apartados número 74 y 75 que, "aunque la mera memorización, por el empresario, de datos nominales relativos a las retribuciones abonadas a su personal no puede, como tal, constituir una injerencia en la vida privada, la comunicación de tales datos a un tercero, en el caso de autos, a una autoridad pública, lesiona el derecho al respeto de la vida privada de los interesados, sea cual fuere la utilización posterior de los datos comunicados de este modo, y presenta el carácter de una injerencia en el sentido del artículo 8 del CEDH"[275]. A lo que añade para confirmarlo que "para demostrar la existencia de tal injerencia, carece de relevancia que los datos comunicados tengan o no carácter sensible o que los interesados hayan sufrido o no eventuales inconvenientes en razón de tal injerencia, basta con observar que el empleador ha comunicado a un tercero los datos relativos a los ingresos que percibe un trabajador o un pensionista".

Sobre este planteamiento, señala además en el apartado número 82, que "procede comprobar, además, si la injerencia de que se trata es necesaria, en una sociedad democrática, para alcanzar la finalidad legítima perseguida", a lo que responde en el apartado número 90 que efectivamente "procede declarar que la injerencia derivada de la aplicación de una normativa nacional como la controvertida en los asuntos principales

[274] Tribunal de Cuentas Alemán. Las entidades sujetas a su control son las territoriales, los organismos de seguridad social, los organismos de representación de intereses profesionales establecidos por ley, un organismo público de radiodifusión (ÖRF), y otras empresas públicas.

[275] Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales. Artículo 8. Derecho al respeto a la vida privada y familiar.
"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

solamente al amparo del artículo 8, apartado 2, del CEDH, en la medida en que la amplia divulgación no sólo del importe de los ingresos anuales, cuando éstos superan un límite determinado, de las personas empleadas por entidades sujetas al control del Rechnungshof, sino también de los nombres de los beneficiarios de dichos ingresos, sea a la vez necesaria y apropiada para lograr el objetivo de mantener los salarios dentro de unos límites razonables, extremo que ha de ser examinado por los órganos jurisdiccionales remitentes". Una vez más, concretando detalles, el TJCE se pronuncia sobre la necesidad de ponderar los derechos en conflicto a la hora de determinar los límites al derecho a la protección de datos personales como derecho fundamental.

Y, por último, la cuarta de las resoluciones, la Sentencia Rundfunk (2003), se pronunciaba sobre el acceso a la información y la garantía de la transparencia, en el tratamiento de datos personales, en relación con medidas que constituyan una injerencia de la autoridad pública en la vida privada de las personas. Señala que una injerencia de este tipo es posible en tanto esté "prevista por una ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás", es decir, que puede justificarse al amparo del artículo 8.2 del CEDH, y laque la Directiva no se opone al principio de transparencia y acceso a la información, pero que éste debe tener muy en cuenta el derecho a la protección de datos personales .

Los países miembros de la Unión Europea, lógicamente han recogido este testigo del TJCE y de las instituciones que rigen la unión política y económica a que pertenecen, y no sólo, en un principio, algunos de ellos también realizaron aportaciones esenciales para entender lo que hoy significa "protección de datos" en el contexto europeo.

La primera norma aprobada, con expresa referencia a la protección de datos de carácter personal, fue la "Datenschutz" de 7 de octubre de 1970 del Estado de Hesse, en la República Federal Alemana. Este texto se dirigía

principalmente a ordenar la actividad de la Administración Pública en lo relativo al tratamiento de bancos de datos, e instituía un "Comisario para la protección de Datos" para supervisar estos procedimientos. Este fue el punto de partida para otras normas de igual carácter surgidas en otros territorios de la R.F.A. y, para la "Datenschutz" estatal (de 1978 primero y de 1986 después), que se promulgaba con alcance tanto sobre el sector público como sobre el sector privado. En esta primera etapa otra norma de similares características, pero publicada fuera del territorio alemán, fue la "Data Lag" sueca de mayo de 1973.

En 1977 se aprobó en la R.F.A. la Ley de 27 de enero de Protección de Datos, conocida por sus siglas "BDGS", que luego ha sido sustituida por un nuevo texto en 1990, y por otro en el año 2001. Siguen a ésta en la promulgación de sus propias leyes Francia, Dinamarca y Austria, en 1978 y, Luxemburgo, en 1979. Con este panorama, se puede afirmar que comenzada la década de los ochenta existía ya cierto reconocimiento a nivel internacional de las facultades jurídicas de la "libertad informática", incluso, que empezaba a consolidarse.

Mientras se configuraba el germen de la protección de datos en el seno institucional de la UE, otros Estados se habían ido sumando a la iniciativa reguladora de la protección de datos. Así, el Reino Unido promulgaba en 1984 la "Data Protection Act"; en Finlandia, se promulgaba en 1987la Ley Nº 471; en Holanda, se promulgaba en 1988 la Ley sobre protección de datos; en Alemania se actualizó 1990 la "BDSG" en este mismo sentido y, en Portugal la primera norma legal de desarrollo no se publicó hasta 1991, a pesar de que en su Constitución estaba previsto específicamente en el artículo 26.3 desde el año 1977.

2.5.- El espacio constitucional europeo.

Los países miembros de la Unión Europea se han ido dotando de normativa específica en esta materia, basándose en sus propios mandatos constitucionales, hasta lograr una armonización legislativa casi generalizada[276]. Así, se ha buscado la homogeneización de las políticas aplicables con el derecho comunitario, hasta el punto de llegar a configurarse una "Constitución Europea" que trata de superar la individualidad de las naciones que la han nutrido.

Esta comunidad política actúa sobre la singularidad nacional generando unidad para un nuevo ámbito de armonización constitucional. Los Estados miembros de la Comunidad Europea se han aproximado asumiendo voluntariamente una autolimitación de sus soberanías y, renunciando a un espacio de poder político, pero a su vez, participando como co-actores del Derecho Comunitario.

CRUZ VILLALÓN, señalaba que en el ámbito de la Unión cabe comprobar la presencia de tres fenómenos de armonización constitucional: "el elemento de la convergencia principal bajo la forma de un "mandato de constitucionalidad"; el elemento de la singularidad garantizado bajo la figura de la "identidad nacional"; y el elemento, por fin, de una convergencia funcional adicional como consecuencia de una "política constitucional" de la Unión, con repercusión sobre los ordenamientos constitucionales nacionales"[277].

Desde que se firmara el Tratado de Maastrich el 7 de Febrero de 1992 (TUE), la UE ha orientado sus políticas en el sentido descrito. En el artículo 6.1 (versión consolidada[278]) se describe la constitucionalidad de la UE en su conjunto: "La Unión reconoce los derechos, libertades y principios

[276] Se puede consultar un listado completo en la sección de "Enlaces de Interés" de la página web de la Agencia Española de Protección de Datos (www.agpd.es).
[277] *La Constitución inédita: Estudios ante la constitucionalización de Europa*. Ed. Trotta. Madrid, 2004. p.55.
[278] Texto disponible en: http://www.boe.es/aeboe/consultas/enlaces/union_europea.php

enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados". Y en el apartado tercero lo confirma al señalar que "Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales".

Se recoge el respeto a la identidad nacional de los Estados miembros, como un ámbito independiente de la integración, pero que sin embargo, forma parte de la Unión, y por ello, se consideró posible instaurar un régimen constitucional común, por medio del "Tratado por el que se establece una Constitución para Europa"[279], a pesar de que Francia y Holanda dijeran "no" en sendos referéndum en el año 2005.

En este sentido, y respecto a la materia que nos ocupa, los países europeos han reconocido la existencia del derecho a la protección de datos de carácter personal, a través de sus Constituciones, de forma más o menos literal o, le han dado forma a través de la jurisprudencia de sus Tribunales Constitucionales (por ejemplo, Alemania, España o Italia), pero todos han ido enfocando las doctrinas con un mismo objetivo: proteger un tratamiento de informaciones personales que se produce con alcance y consecuencias internacionales.

Centrándonos en los textos constitucionales de los Estados miembros, el primero en reconocer expresamente la necesidad de proteger este ámbito de la vida privada fue la Constitución portuguesa[280] de 1976:

[279] "INSPIRÁNDOSE en la herencia cultural, religiosa y humanista de Europa, a partir de la cual se han desarrollado los valores universales de los derechos inviolables e inalienables de la persona humana, la democracia, la igualdad, la libertad y el Estado de Derecho. (...) CONVENCIDOS de que los pueblos de Europa, sin dejar de sentirse orgullosos de su identidad y de su historia nacional, están decididos a superar sus antiguas divisiones y, cada vez más estrechamente unidos, a forjar un destino común. (...) DECIDIDOS a continuar la obra realizada en el marco de los Tratados constitutivos de las Comunidades Europeas y del Tratado de la Unión Europea, garantizando la continuidad del acervo Comunitario". Preámbulo. DOUE (16/12/2004).

[280] Texto disponible en (portugués): http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx

En el artículo 26.1 recogió la previsión general de que "La ley establecerá garantías efectivas contra la utilización abusiva, o contraria a la dignidad humana, de informaciones relativas a las personas y a las familias". Y de forma más precisa, se expresa en el artículo 35: "Utilización de la informática.

> 1. Todos los ciudadanos tienen el derecho a acceder a sus datos informatizados, pudiendo exigir su rectificación y actualización, y el derecho de conocer la finalidad a que se destinan, en los términos de la Ley.
>
> 2. La ley definirá el concepto de datos personales, así como las condiciones aplicables a su tratamiento automatizado, conexión, transmisión y utilización y, garantizará su protección a través de la entidad administrativa independiente designada.
>
> 3. La informática no puede ser utilizada para el tratamiento de datos relativos a convicciones ideológicas o políticas, afiliación sindical, creencias religiosas, vida privada u origen étnico, salvo que medie consentimiento expreso del titular, autorización legalmente prevista con garantías de no discriminación o, lo sea para el procesamiento de datos estadísticos no identificables individualmente.
>
> 4. Está prohibido el acceso a los datos personales de terceros, salvo en casos excepcionales previstos por la Ley.
>
> 5. Está prohibido la atribución de un número nacional único a los ciudadanos.
>
> 6. Se garantiza el libre acceso a las redes informáticas de uso público, definiendo la Ley el régimen aplicable a los flujos de datos transfronterizos y, las formas adecuadas de

protección de datos personales y de otros cuya salvaguarda se justifique por razones de interés nacional.

7. Los datos personales permanentes de ficheros manuales, gozan de protección idéntica a la prevista en los números anteriores, en los términos de la Ley".

De este precepto, destaca especialmente lo relativo a los ficheros de datos manuales, es decir, desvincula la protección de datos no sólo de la intimidad, sino también de la informática. Esto es algo tan relevante como extraño en lo que a textos constitucionales se refiere, porque la línea general seguida en Europa parte de la protección de la intimidad, del domicilio y de las comunicaciones, como garantía para la protección de la información personal, es mantenerlo en relación directa con ambos conceptos. También resulta llamativa la prohibición del número identificador único para los ciudadanos, que sin embargo, es admitido sin reservas en otros países como España.

Otra constitución europea relevante, por cómo se interpretó su contenido, es la Ley Fundamental de la República Federal Alemana[281], de 23 de Mayo de 1949. De ella surgió la dimensión constitucional de la protección de los datos personales que conocemos hoy en Europa, a través de la valoración que el Tribunal Constitucional Federal alemán hizo sobre el derecho general de la personalidad, de la dignidad de la persona y de su libre desarrollo, en la Sentencia de 15 de Diciembre 1983 sobre la Ley del censo, de 4 de marzo de 1982. El artículo 2 señala: "Toda persona tiene el derecho al libre desarrollo de su personalidad siempre que no viole los derechos de otra ni atente contra el orden constitucional o la ley moral. Toda persona tiene el derecho a la vida y a la integridad física. La libertad de la persona es inviolable. Estos derechos sólo podrán ser restringidos en virtud de una ley".

[281] Página web oficial de la Constitución Europea: http://www.constitucion.es/otras_constituciones/europa/index.html

Con esta previsión se trata de asegurar un ámbito de la personalidad del individuo que le permita disfrutar su libertad y dirigir su propia capacidad de decisión, frente al abuso de quienes realizan tratamientos de datos personales. Es decir, la dignidad (y la libertad como parte de ésta) se pone de manifiesto como sustrato esencial de la protección de datos personales.

La mayoría de la doctrina y jurisprudencia en Europa ha evolucionado en torno al concepto "intimidad" como continente del derecho a la protección de datos, y en ello se basan precisamente constituciones como la de España, Bélgica[282], Chipre[283], Dinamarca[284], Finlandia[285], Hungría[286], Luxemburgo[287] o Paises Bajos[288]. Mención aparte merecería el caso de Irlanda, porque su texto constitucional, que entró en vigor en 1937, y ha sido objeto de múltiples enmiendas, centra la protección de la intimidad

[282] El primer texto de la Constitución belga data de 1831. Tras varias reformas (en 1970, 1980, 1988 y 1993), el 17 de febrero de 1994 se publicó la "Constitución refundida", que sistematiza las anteriores. Fue modificado por última vez en el año 2002. La Ley de Bélgica de protección de la privacidad con respecto al procesamiento de los datos personales, es de fecha 9 de diciembre de 1992. de 1994, habla de "vida privada", señalando en su artículo 22 que cada uno tendrá derecho al respeto de su vida privada y familiar, salvo en los supuestos y con las condiciones establecidas por la ley.

[283] En 1959 Chipre firmó el Acuerdo de independencia con Inglaterra y, desde entonces cuenta con su propio texto constitucional. El texto se presentó por la Comisión constitucional al Parlamento Británico, y fue aprobado en 1960. Consta de 21 Apéndices. de 1960, también se refiere a la "intimidad" en su artículo 15 , que es reforzado por los artículos 16 y 17, sobre la inviolabilidad del domicilio y el secreto de las comunicaciones, respectivamente.

[284] Al finalizar la Segunda Guerra Mundial, Dinamarca se planteó distintas reformas en su texto constitucional, finalmente, en 1953 se aprobó el texto actual, que se mantiene sin cambios. Centra su articulado en la definición de los poderes estatales, el Rey y el Parlamento (Folketing), pero si recoge sin embargo, como "derechos individuales" la inviolabilidad del domicilio y de las comunicaciones (artículo 72).

[285] El primero texto constitucional de la República de Finlandia, data de 1919, pero el actual fue sancionado en Helsinki el 11 de Junio de 1999, y entró en vigor en el año 2000, y es en el artículo10 en el que se garantiza la "privacidad": "la intimidad, el honor personal, la inviolabilidad del domicilio, el secreto de las comunicaciones y, señala expresamente en su primer apartado que la protección de los datos personales estará regulada más precisamente por Ley".

[286] La Constitución de Hungría actual entró en vigor el 1 de Enero de 2012, recuperando la tradición cristiana del país y, cambiando su nombre oficial, que ha pasado de llamarse República Húngara. Esta nueva norma recoge su protección al derecho a la "vida privada" el artículo VI *(1)* "Toda persona tendrá derecho a la protección de su familia y la privada de la vida, el hogar, las relaciones y la buena reputación. (2) Toda persona tendrá derecho a la protección de sus datos personales, y para acceder y difundir datos de interés público. (3) El ejercicio del derecho a la protección de los datos personales y el acceso a los datos de interés público deberán ser supervisadas por una autoridad independiente. El texto, actualizado sobre el original del año 1949, es de la última reforma habida, en el año 2012".

[287] En Luxemburgo, existe una de las constituciones más antiguas de la Unión Europea (1868) e, incluyendo la creación de un Tribunal Constitucional en 1996, ha pasado por distintas reformas, y también reconoce el "derecho a la intimidad", a través de la protección de los tradicionales domicilio y comunicaciones (arts. 14 y 18).

[288] La Constitución de los Países Bajos, de 17 de febrero de 1983 (que es una revisión completa de la de 1815), se caracteriza por no incluir un sistema de control de constitucionalidad para las leyes, porque otorga (artículo 92 y siguientes) prioridad a las aplicabilidad de las normas de Derecho internacional. Sin embargo, contiene una previsión expresa en materia de protección de datos personales , diciendo (artículo 10) que la ley establecerá normas referentes al derecho de toda persona a conocer los datos registrados que le afecten y su utilización, así como a poder rectificarlos.

del individuo en la protección de la familia como institución fundamental del Estado[289]. Reconoce "que será inviolable el domicilio de todo ciudadano y no se podrá entrar por la fuerza en el sino de acuerdo con lo dispuesto en la ley, sin embargo, lo relativo a la protección de la familia" (artículo 40.5), y su Ley de protección de datos, que data de 1988 (modificada en el año 2003) basa sus previsiones en el concepto de esa "vida privada" y familiar. Y más llamativo es aún, que este país haya llegado incluso a considerar que la Constitución del Estado está por encima de la Convención Europea de Derechos Humanos, en cuanto al respeto a la vida privada, pero una Sentencia del TEDH de 16 de Diciembre de 2010, en relación con el aborto (las leyes pro-vida de Irlanda violaban el derecho a la privacidad del CEDH), ha obligado a rectificar estas consideraciones en el sentido del más absoluto respeto a las previsiones de dicho Convenio.

Otros Estados Miembros, por el contrario, han ido adaptando el Derecho Comunitario aplicable en esta materia, partiendo del concepto de "libertad".

Por ejemplo, la Constitución Federal Austríaca[290] ("Osterreichische Bundesverfassung") de 1920, que con KELSEN[291] consagró el control jurisdiccional por el "Tribunal Constitucional" en materia de derechos fundamentales, remite lo relativo a la protección de datos a la protección de la "libertad personal" a través de su Anexo "Leyes Constitucionales

[289] Artículo 41 de la Constitución Irlandesa:
"1. 1º. El Estado reconoce a la familia como el grupo unitario natural, primario y fundamental de la sociedad y como institución moral poseedora de derechos inalienables e imprescriptibles, anteriores y superiores a toda ley positiva.
2º. El Estado se compromete, por lo tanto, a proteger la familia en su constitución y autoridad como base necesaria del orden social y como indispensable al bien de la Nación y del Estado.
2. 1º. En particular, el Estado reconoce que con su vida dentro del hogar la mujer brinda al Estado un apoyo sin el cual no se podría conseguir el bien común.
2º. El Estado se esforzara, por consiguiente, en garantizar que las madres no se vean obligadas por necesidades económicas a dedicarse al trabajo con descuido de sus deberes en el hogar.
3. 1º. El Estado se compromete a preservar con especial solicitud la institución del matrimonio (marriage), en la que se basa la familia, y a protegerla contra todo ataque.
2º. No se elaborara ley alguna que prevea la disolución del matrimonio.
3º. Ninguna persona cuyo matrimonio haya quedado disuelto con arreglo al derecho civil de algún otro Estado pero siga siendo un matrimonio valido conforme al ordenamiento vigente bajo la jurisdicción del Gobierno y del Parlamento establecidos por esta Constitución, podrá contraer matrimonio valido dentro de dicho ámbito de jurisdicción mientras continué viviendo la otra parte del matrimonio así disuelto".
[290] Promulgada en 1920, ha sido reformada por más de treinta leyes constitucionales. La última, es del año 2008. Especialmente importante es la reforma de 1994, en que se adaptó el derecho constitucional austriaco al Tratado de la Unión Europea.
[291] H.Kelsen fue magistrado de la Corte Constitucional austriaca desde 1921 hasta 1929. GARCÍA DE ENTERRÍA, E. *La Constitución como norma*... Op.Cit. p.56.

Declaradas Vigentes". Aparte, además, otorga al Convenio Europeo de Derechos Humanos de 1950 el valor de norma constitucional federal, recogiendo en su artículo 8 que el "derecho al respeto a la vida privada y familiar" es directamente aplicable sobre el derecho interno.

Esta misma idea ya la proclamaba la Constitución francesa de 3 de Septiembre de 1791, que regulaba en su Título Primero las "Disposiciones Fundamentales Garantizadas por la constitución", y decía que el Poder Legislativo no podía hacer leyes que vulneren o pongan trabas al ejercicio de los derechos naturales o civiles consignados en ese título, garantizados por la Constitución[292]. Sin embargo, señala también que, como la libertad no consiste más que en poder hacer todo aquello que no perjudique ni a los derechos de los demás ni a la seguridad pública, la Ley podrá establecer penas contra los actos que, atentando contra la seguridad pública o los derechos de los demás, fueren perjudiciales para la sociedad. Italia[293], Grecia[294] y Suecia[295], entienden igualmente el libre desarrollo de la

[292] En el año 2008 el pueblo francés actualizó su Constitución, señalando expresamente en el Preámbulo que el pueblo francés proclamaba solemnemente su adhesión a los derechos humanos y a los principios de la soberanía nacional tal y como fueron definidos por la Declaración de 1789, confirmada y completada por el Preámbulo de la Constitución de 1946, dejando la protección de la "privacidad" al Código Civil, bastando con reconocerle garantías procesales

[293] La Constitución de Italia de 1947, aprobada por la Asamblea Constituyente de 22 de diciembre 1947 consagra los valores democráticos y establece un Estado nacional, soberano, independiente, unitario y indivisible, ha sufrido diferentes reformas, y el último intento (frustrado) fue en el año 2007. Recoge los tradicionales preceptos relativos a la "intimidad": a la inviolabilidad del domicilio y al secreto de las comunicaciones (artículos 14 y 15), y la doctrina ha analizado este derecho a la "riservatezza" como un elemento de la libertad personal. Es uno de los países con una doctrina más concienciadora en materia de protección de datos, y su adaptación a los cambios es continua, así, por ejemplo, la Directiva 95/46/CE se incorporó al derecho interno mediante el Codice in materia di protezione dei dati personali, de 30 de junio del 2003, que ha vuelto a ser modificado en el año 2012: Modificado por el Decreto Legge 9 febbraio 2012, n. 5. "Disposizioni urgenti in materia di semplificazione e di sviluppo (Gazzetta Ufficiale n. 33 del 9 febbraio 2012): Artículo 45 Semplificazioni in materia di dati personali.
1. Al decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:
a) all'articolo 21 dopo il comma 1 è inserito il seguente:
1-bis. Il trattamento dei dati giudiziari è altresì consentito quando è effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con i suoi uffici periferici di cui all'articolo 15, comma 2, del decreto legislativo 30 luglio 1999, n. 300, che specificano la tipologia dei dati trattati e delle operazioni eseguibili."; b) all'articolo 27, comma 1, è aggiunto, in fine, il seguente periodo: "Si applica quanto previsto dall'articolo 21, comma 1-bis."; c) all'articolo 34 è soppressa la lettera g) del comma 1 ed è abrogato il comma 1-bis; d) nel disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B sono soppressi i paragrafi da 19 a 19.8 e 26".
Algunas obras en esta materia: Privacy e giornalismo. Diritto di cronaca e diritti dei cittadini de Mauro Paissan, Italia, 2007; La protezione dei dati personali de Giuseppe Santaniello, Italia, 2005; Da costo a risorsa, la privacy come elemento qualitativo per l'impresa de Gaetano Rasi, Italia, 2004; Ideologie e tecniche della riforma del diritto civile, Italia, 2007 y Dal soggetto alla persona, Italia, 2007, estos dos últimos del que fuera Presidente dell'Autorità garante per la protezione dei dati personali (1997-2005) y Presidente del Gruppo dei garanti europei (2000-2004), el Profesor Stefano Rodotà.

[294] En 1975, terminado definitivamente el régimen militar y abolida la monarquía por referéndum popular, Grecia se dotó de una Constitución republicana y democrática. Recoge en un primer artículo una previsión genérica sobre el "respeto a los individuos" y, algo más específicamente, dice en su artículo 5 que cada uno tendrá derecho a desarrollar libremente su personalidad y a participar en la vida social, económica y política del país con tal que no atente a los derechos de los demás ni viole la Constitución ni

personalidad como la justificación de toda medida protectora de la intimidad o, en su caso, la protección del derecho a la protección, siendo que esta última además realiza una distinción expresa de los tres derechos fundamentales.

En otro orden de cosas, en cuanto a aportaciones constitucionales de naturaleza jurisprudencial en los Estados miembros, al contenido del derecho a la protección de datos personales, el Tribunal más creativo ha sido el Tribunal Constitucional Alemán. La Sentencia de mayor relevancia, por novedosa, fue la Sentencia de 1983 sobre el censo poblacional, aunque ha habido otras posteriores, como por ejemplo la Sentencia de 27 de Febrero de 2008. Esta resolución, es resultado de un recurso interpuesto contra la reforma de la Ley de los Servicios de Inteligencia del Estado Federal de Renania del Norte Westfalia, que permitía los registros ocultos "online" de ordenadores de cualquier persona sospechosa de terrorismo. No se trataba de proteger el secreto de las comunicaciones, sino datos que han sido almacenados, como un derecho general de la personalidad El Tribunal reclama la protección de la confidencialidad e integridad de los sistemas tecnológicos de información, y dice: de la relevancia del uso de los sistemas tecnológicos de información para expresar la personalidad y de los peligros que para la personalidad representa tal uso, deriva una necesidad de protección que es significativa para los derechos fundamentales. El individuo depende de que el Estado respete las expectativas justificables de confidencialidad e integridad de tales sistemas de cara a la absoluta expresión de su personalidad. Y ya hay quien lo ha reconocido como el derecho a la garantía de la confidencialidad e integridad de los sistemas técnicos de información (Protección de Ordenadores).

---

las buenas costumbres. Esta previsión se complementa con lo dispuesto en el artículo 9: "El domicilio personal se considera como un asilo. Es inviolable la vida privada y familiar de la persona. No se podrá efectuar registro domiciliario alguno sino en los casos y de la forma determinada por la ley, y siempre en presencia de representantes del poder judicial". La Ley 2472/1997 incorporó la Directiva 95/46/CE a la legislación griega, y creó la Autoridad Helénica de Protección de Datos. Desde su aprobación, la Constitución ha sido revisada en tres ocasiones: en 1986, 2001 y 2008.

[295] La Constitución de Suecia de 1974 es uno de los textos más liberales de Europa, su Capítulo II recoge todo lo relativo a los derechos fundamentales y, es el tercer precepto de este capítulo el que declara expresamente la libertad de los ciudadanos para "decidir sobre su propia información personal" y, el derecho a que ésta goce de la protección y garantías que merece: Ningún dato sobre un ciudadano recogido en registros públicos podrá basarse sin su consentimiento, exclusivamente en sus opiniones políticas. Se protegerá a los ciudadanos en la medida precisada por la ley contra cualquier lesión de su integridad personal resultante del almacenamiento de datos que les afecten, mediante tratamiento informático. Además de esta previsión específica, también recoge (artículo 6) la inviolabilidad domiciliaria y el secreto a las comunicaciones.

La confidencialidad de un sistema tecnológico, sólo debe ser limitada a causas muy concretas, es decir, si hay "hechos concretos" que apuntan a un peligro inminente, como sería en caso de riesgo evidente para la vida, la integridad física o la libertad de las personas, así como para los pilares del Estado o los poderes públicos. No es posible utilizar estas técnicas de registro mediante spyware por los servicios de inteligencia de forma genérica, independientemente de que el particular no sea en principio el destinatario como tal, sino como parte de una generalidad indeterminada, porque con ello si se afectarán aspectos de su vida privada que nada tiene que ver con el fin de la concreta investigación, y generaría una atmósfera de intimidación hasta provocar el efecto disuasivo de no querer ejercer el derecho fundamental. Se reconoce que la tecnología es parte de la vida personal de los ciudadanos, y que requiere ser protegida, evitando dejar en manos del estado la posibilidad de realizar perfiles de comportamiento, relaciones o sentimientos, pues este tipo de sistemas de vigilancia conducen a un acoso general sobre el libre desarrollo de la personalidad.

Así mismo, es importante la Sentencia de 2 marzo de 2010, invalidando la Ley de Acopio y Almacenamiento de Datos. El Tribunal declaró nulos, por violación del derecho al secreto de las comunicaciones, los preceptos legales que traspusieron la Directiva 2006/24/CE sobre conservación de datos asociados a las mismas. la nulidad de los § 100 g) del Código Procesal Penal y 113 a) y b) de la Ley Federal de Telecomunicaciones, introducidos por la Ley de 21 de diciembre de 2007. En particular, infringía el artículo 10.1 de la Ley Fundamental de Bonn (secreto de las comunicaciones y derecho a la autodeterminación informativa), ya que establecieron la obligación de "los proveedores de servicios de telecomunicaciones accesibles públicamente de conservar todo el tráfico de datos de las comunicaciones por teléfono (fijo y móvil), fax, SMS, MMS, correo electrónico y de los servicios de Internet" (quién realizaba o intentaba la comunicación, cuándo, por cuánto tiempo, con quien, desde dónde, etc., pero no su contenido), y las finalidades serían "la persecución de las infracciones criminales, la prevención de peligros sustanciales para la seguridad pública y el cumplimiento de las funciones de los servicios de inteligencia". La cuestión sometida al Tribunal fue la falta de proporcionalidad entre la medida y los

fines, y que los datos almacenados "podían ser usados para crear perfiles de personalidad y para rastrear los movimientos de las personas". Los argumentos principales[296] fueron estimados por la sentencia.

3.- Las garantías: "El ciudadano de cristal":

3.1.- Ejercicio de derechos y transparencia.

La Real Academia Española de la Lengua define el término "libertad" (primera acepción), como "la facultad natural que tiene el hombre de obrar de una manera o de otra, y de no obrar, por lo que es responsable de sus actos" y, se ha dicho en varios apartados que el artículo 18.4 de la CE defendía en principio la "libertad (en relación con la) informática" o, más ampliamente, el "derecho a la autodeterminación informativa", y que son conceptos acuñados para informar sobre la garantía de la protección de datos personales. Para integrar esa libertad en el contexto informático, se estableció el correspondiente marco legal exigiera responsabilidades y detallase los extremos y circunstancias que se han de dar para su efectivo ejercicio, como derecho fundamental.

El Tribunal Constitucional planteó considerar la protección de datos como un derecho fundamental[297] exclusivo y, entendió la necesidad de

[296] LUCAS MURILLO DE LA CUEVA, P. "Novedades sobre el derecho a la protección de datos personales". Fundación Ciudadanía y valores. Curso de Verano: *Organismos Internacionales y nuevo orden mundial*. Aranjuez, 2010. p. 14. Disponible en: http://www.funciva.org/uploads/ficheros_documentos/1284377010_pablo_lucas.pdf

[297] STC 202/1999, sobre el tratamiento de datos de salud del trabajador sin su consentimiento expreso (F.Jº. 2º). Respecto del artículo 18.4 CE: "Se trata, por tanto, de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo,

dotarlo de protección legal eficaz frente al uso de la informática, porque el artículo 18.4 consagraba[298] el derecho de los individuos a protegerse de los tratamientos ilegítimos de su información personal, y requería una regulación autónoma que permitiese hacerlo efectivo.

El desarrollo normativo del artículo 18. 4 de la CE, tiene pues la misión de procurar eficacia material al "haz de facultades" que lo compone, para que los ciudadanos puedan exigir, desde una posición activa, la protección de su propia información personal, y que se ha traducido en la práctica en diferentes aspectos: en el derecho a ser informado de los tratamientos que se realicen con sus datos, a negarse a proporcionar más información de la estrictamente necesaria, a acceder a esa información, a pedir que se rectifique o se cancele, a exigir que dicho tratamiento se realice con la debida confidencialidad (medidas de seguridad que eviten toda alteración, pérdida o acceso no autorizado), a revocar su consentimiento en cualquier momento, a oponerse a que sea cedida, etc[299].

Y también, para exigir responsabilidades en caso de manipulaciones por terceros no autorizados, cuentan con el oportuno sistema de resolución de conflictos y tutela de derechos[300], de carácter administrativo, que se desarrolla al amparo de la una autoridad de control independiente, que es la Agencia de Protección de Datos[301]. Además, finalizada esta vía de reclamación, cuentan con la vía jurisdiccional contencioso – administrativa para impugnar las decisiones de esa entidad y, con la vía jurisdiccional civil, para exigir las indemnizaciones que pudiera corresponder.

---

un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos (SSTC 254/1993, F.Jº. 6º, y 11/1998, F.Jº. 4º)".

[298] La STC 11/1998 (F.Jº. 6º), utiliza esta palabra para establecer que el artículo 18.4 CE además de suponer una garantía frente al uso de la informática, entraña un derecho fundamental autónomo e independiente de la intimidad Según el Diccionario de la Real Academia de la Lengua, consagrar significa "conferir a alguien o algo fama o preeminencia en determinado ámbito o actividad", lo que necesariamente implica que para que algo pueda ser consagrado, debe existir con anterioridad, y así se defiende respecto del Derecho a la Autodeterminación Informativa, como derecho de libertad y dignidad humana.

[299] Artículos 4 a 19 de la LOPD.

[300] Artículo 48 de la LOPD.

[301] Artículo 35 de la LOPD.

El Tribunal Constitucional ha interpretado que el artículo 18.4 de la CE es un "instituto de garantía", pero que también es un instituto que "es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática", lo que se ha dado en llamar "libertad informática" (F.Jº. 6º, reiterado luego en las SSTC 143/1994 F.Jº. 7º, 11/1998 FJ 4, 94/1998 F.Jº. 6º, 202/1999 F.Jº. 2º)", y establece que ésta debe considerarse como el "derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención"[302]. Se trata de salvaguardar un aspecto concreto de la libertad y simplemente, la considera en relación con la informática.

La Declaración de los Derechos del Hombre y del Ciudadano de 1789, decía en su artículo cuarto que la "libertad" consiste en "poder hacer todo aquello que no perjudique a los demás y al tener en cuenta que el ejercicio de los derechos naturales de cada hombre no tiene otra limitación que aquella que garantice el ejercicio de iguales derechos al resto de los miembros de la sociedad. Sólo la ley puede establecer estas limitaciones".

El ejercicio del derecho a la protección de datos no es absoluto, no prevalece frente a otras libertades, de otros ciudadanos, y es un reto para el Estado de Derecho coordinar equilibradamente los parámetros que lo hacen eficaz y los que lo limitan, sin perjudicar su estabilidad.

Hasta ahora se ha tratado la confidencialidad de la información de los ciudadanos, como una parte esencial de su personalidad, un derecho (o un "haz de facultades") sin el cual no podría hablarse ni de libertad ni de seguridad. Sin embargo, si se aplica esta máxima como una verdad absoluta e ilimitada, lo cierto es que podemos caer en la falsa consideración de que

[302] STC 292/2000, sobre la delimitación del derecho fundamental a la protección de datos e inconstitucionalidad de ciertos incisos de la LO 15/1999, en su F.Jº. 5º, haciendo referencia a las SSTC 254/1993, 94/1998 y 202/1999.

solo hay estado democrático si se protege la información de los ciudadanos, con opacidad absoluta frente al Estado.

Está claro que la seguridad estatal no puede ser carta blanca para configurar el Estado como un conjunto de "ciudadanos de cristal", pero la protección de datos tampoco puede ser carta blanca para que los poderes públicos (quienes los gobiernan), puedan ocultar su actividad ilimitadamente. La transparencia también es esencial para poder hablar de un Estado Democrático, el reconocimiento y garantía del derecho de los ciudadanos a acceder a la información pública, es una práctica de buen gobierno[303].

Este derecho tiene sus antecedentes más remotos y conocidos en la Real Ordenanza sobre Libertad de Prensa sueca de 1766, y en la Declaración de Derechos del Hombre y el Ciudadano de 1789 (artículo 15), que proclamaba que la sociedad tiene derecho a pedir cuentas de su gestión a todo agente público". Pero no será hasta la década de los sesenta cuando empiece a extenderse de una forma generalizada. Pioneros fueron los Estados Unidos con la Freedom of Information Act de 1966, y algunos países del norte de Europa, como Finlandia, donde el derecho estaba reconocido desde 1951, o Dinamarca y Noruega, dos leyes de 10 y 19 de junio de 1970 respectivamente. Francia, con una ley de 17 de julio de 1978, Gan Bretaña, con las recomendaciones de la Comisión Franks de 1972 (y la reforma de la Ley de Secretos Oficiales, en 1989), o Italia, con una Ley de 7 de agosto de 1990.

La mayoría de los Estados Miembros cuentan con legislación específica en esta materia, y en el Derecho comunitario (el derecho de acceso, como derecho autónomo vinculado con el principio democrático y el derecho de participación de los ciudadanos en los asuntos públicos, con la obligación de transparencia y con la libertad de información) lo reconocen el Tratado de Funcionamiento de la Unión Europea y la Carta de los Derechos Fundamentales de la Unión Europea, y lo desarrolla el Reglamento (CE) n°1049/2001 de 30 de mayo de 2001, relativo al acceso del público a los

[303] Exposición de Motivos de la versión del Anteproyecto de ley de transparencia y acceso de los ciudadanos a la información pública. Ministerio de la Presidencia, de fecha 17 de Agosto de 2010.

documentos del Parlamento Europeo, del Consejo y de la Comisión. Además, el Convenio Europeo sobre Acceso a los Documentos Públicos del Consejo de Ministros del Consejo de Europa, el 27 de noviembre de 2008, que constituye el primer instrumento jurídico internacional vinculante que reconoce un derecho general de acceso a los documentos públicos y recoge los principios inspiradores de la Recomendación Rec (2002)2 del Comité de Ministros a los Estados Miembros sobre acceso a los documentos públicos. Ambos textos parten del convencimiento de que, "al garantizar el ejercicio del derecho de acceso a los documentos públicos, se dota a los ciudadanos de una fuente de información que contribuye a formar opinión sobre los problemas de la sociedad y el comportamiento y la actividad de las autoridades públicas, y se favorece la integridad, el buen funcionamiento, la eficacia y la responsabilidad de éstas, todo lo cual juega en incremento de su legitimidad"[304].

Según el Supervisor Europeo de Protección de Datos (Dictamen de Julio de 2005), la transparencia hace referencia a tres elementos y sus características: "el proceso de elaboración de decisiones por los entes públicos que ha de ser abierto y participado; las decisiones que deben ser motivadas y razonables; la información que sirve de base a la adopción de decisiones debe ser, en la medida de lo posible, accesible al público". Asimismo, en caso de conflicto con el derecho a la protección de datos habrá de valorarse si la vida privada de la persona está en juego, si el ejercicio del derecho de acceso afecta a la persona en cuestión, y si la legislación específica en materia de protección de datos impide la comunicación (debe verse si afectar a la esfera privada e íntima de la persona, como por ejemplo, información sobre su salud o que afecte a su honor)[305].

En España, el artículo 105.b) de la Constitución de 1978 dice taxativamente que la ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo "lo que afecte" a la "seguridad y defensa

[304] Exposición de Motivos. Apartado II. Ibídem.

[305] *FERNÁNDEZ HEVIA, J.M. Acceso público a la documentación y protección de datos.* "Dictamen del Supervisor Europeo de Protección de Datos". Documentos de Referencia, nº 1. Julio 2005. Boletín de la Asociación Asturiana de Bibliotecarios (AABADOM), 2005 ENE-JUN; XVI. pp. 43 y 44. Disponible en: http://ria.asturias.es/RIA/bitstream/123456789/127/1/supervisor_protecciondedatos.pdf

del Estado, la averiguación de los delitos y la intimidad de las personas"[306]. Pero el derecho de acceso a la información en poder de la Administración no fue regulado[307] hasta 1992, con la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que se reguló este derecho. Dispone en el artículo 3.5 que "en sus relaciones con los ciudadanos las Administraciones públicas actúan de conformidad con los principios de transparencia y de participación". Por otra parte, el artículo 37 señala que "los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud", con las salvedades precisas en lo que pueda afectar a su intimidad[308]. Pero esta Ley, ni otras

[306] Anteriormente, el Texto articulado de la Ley de Funcionarios Civiles del Estado, de 7 de febrero de 1965, ordenaba a los agentes públicos "guardar un sigilo riguroso" respecto de aquellos asuntos que conocieran por razón de su cargo (artículo 80), y no existía ninguna norma sobre la posibilidad efectiva de recabar oficialmente información de la Administración (salvo el expediente, para los "interesados", en un procedimiento administrativo); y la Ley sobre Secretos Oficiales, Ley 9/1968, de 5 de abril, de 1968, abría el principio general de publicidad, salvo para las materias expresamente "clasificadas".

[307] Excepto, leves referencias: en el artículo 70.3 de la Ley de Bases del Régimen Local de 1985, y el artículo 230 del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales de 1986. Y también en la Ley Orgánica de Régimen Electoral General (artículo 41), en la Ley General de Sanidad (artículo 10.3), en la Ley de la Función Pública Estadística (artículo 13), en la Ley General Tributaria (artículo 111), en la Ley del Patrimonio Histórico Español (artículo 27) y en la LOPD, pero más bien, lo que hacen es establecer límites específicos del derecho de acceso para salvaguardar la confidencialidad de datos personales.

[308] Artículo 37. Derecho de acceso a Archivos y Registros. "1. Los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud. 2. El acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas, que, en el supuesto de observar que tales datos figuran incompletos o inexactos, podrán exigir que sean rectificados o completados, salvo que figuren en expedientes caducados por el transcurso del tiempo, conforme a los plazos máximos que determinen los diferentes procedimientos, de los que no pueda derivarse efecto sustantivo alguno. 3. El acceso a los documentos de carácter nominativo que sin incluir otros datos pertenecientes a la intimidad de las personas figuren en los procedimientos de aplicación del derecho, salvo los de carácter sancionador o disciplinario, y que, en consideración a su contenido, puedan hacerse valer para el ejercicio de los derechos de los ciudadanos, podrá ser ejercido, además de por sus titulares, por terceros que acrediten un interés legítimo y directo. 4. El ejercicio de los derechos que establecen los apartados anteriores podrá ser denegado cuando prevalezcan razones de interés público, por intereses de terceros más dignos de protección o cuando así lo disponga una Ley, debiendo, en estos casos, el órgano competente dictar resolución motivada. 5. El derecho de acceso no podrá ser ejercido respecto a los siguientes expedientes: A) Los que contengan información sobre las actuaciones del Gobierno del Estado o de las Comunidades Autónomas, en el ejercicio de sus competencias constitucionales no sujetas a Derecho Administrativo. B) Los que contengan información sobre la Defensa Nacional o la Seguridad del Estado. C) Los tramitados para la investigación de los delitos cuando pudiera ponerse en peligro la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. D) Los relativos a las materias protegidas por el secreto comercial o industrial. E) Los relativos a actuaciones administrativas derivadas de la política monetaria. 6. Se regirán por sus disposiciones específicas: A) El acceso a los archivos sometidos a la normativa sobre materias clasificadas. B) El acceso a documentos y expedientes que contengan datos sanitarios personales de los pacientes. C) Los archivos regulados por la legislación del régimen electoral. D) Los archivos que sirvan a fines exclusivamente estadísticos dentro del ámbito de la función estadística pública. E) El Registro Civil y el Registro Central de Penados y

posteriores sectoriales[309], no fue el remedio a la falta de transparencia en la Administración pública, pues para empezar, restringe el acceso a otros documentos "de carácter nominativo", a terceros que acrediten un interés legítimo y directo, siempre que los datos que contengan puedan hacerse valer para el ejercicio de sus derechos (artículo 37.3). Y si por "documento de carácter nominativo" se entiende que pueda serlo cualquiera que contenga referencias nominales a una o varias personas, el límite a la legitimación para ejercitar este derecho resulta muy restrictivo.

En Agosto del año 2010, el Ministerio de la Presidencia publicó el primer borrador del "Anteproyecto de ley de transparencia y acceso de los ciudadanos a la información pública", que tras ser sometido a consulta pública, en el año 2012 ha pasado a llamarse "Anteproyecto de Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno"[310], y trata de desarrollar el principio constitucional de transparencia, el que reconoce el derecho de acceso a la información pública (artículo 105. 1 b de la CE), reforzado por el derecho a recibir libremente información (artículo 20. 1 d de la CE).

En el apartado I de su Exposición de Motivos, recoge el espíritu de la futura norma y sus triple alcance: "incrementa y refuerza la transparencia en

---

Rebeldes y los registros de carácter público cuyo uso esté regulado por una Ley. F) El acceso a los documentos obrantes en los archivos de las Administraciones Públicas por parte de las personas que ostenten la condición de Diputado de las Cortes Generales, Senador, miembro de una Asamblea legislativa de Comunidad Autónoma o de una Corporación Local. G) La consulta de fondos documentales existentes en los Archivos Históricos. 7. El derecho de acceso será ejercido por los particulares de forma que no se vea afectada la eficacia del funcionamiento de los servicios públicos debiéndose, a tal fin, formular petición individualizada de los documentos que se desee consultar, sin que quepa, salvo para su consideración con carácter potestativo, formular solicitud genérica sobre una materia o conjunto de materias. No obstante, cuando los solicitantes sean investigadores que acrediten un interés histórico, científico o cultural relevante, se podrá autorizar el acceso directo de aquéllos a la consulta de los expedientes, siempre que quede garantizada debidamente la intimidad de las personas. 8. El derecho de acceso conllevará el de obtener copias o certificados de los documentos cuyo examen sea autorizado por la Administración, previo pago, en su caso, de las exacciones que se hallen legalmente establecidas. 9. Será objeto de periódica publicación la relación de los documentos obrantes en poder de las Administraciones Públicas sujetos a un régimen de especial publicidad por afectar a la colectividad en su conjunto y cuantos otros puedan ser objeto de consulta por los particulares. 10. Serán objeto de publicación regular las instrucciones y respuestas a consultas planteadas por los particulares u otros órganos administrativos que comporten una interpretación del derecho positivo o de los procedimientos vigentes a efectos de que puedan ser alegadas por los particulares en sus relaciones con la Administración".

[309] Ley 27/2006, de 18 de Julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente; la Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y la Ley 37/2007, de 16 de Noviembre, sobre reutilización de la información del sector público.

[310] Se puede consultar el texto del Anteproyecto en:
http://www.leydetransparencia.gob.es/anteproyecto/

la actividad pública -que se articula a través de obligaciones de publicidad activa para todas las Administraciones y entidades públicas-, reconoce y garantiza el acceso a la información -regulado como un derecho de amplio ámbito subjetivo y objetivo- y establece las obligaciones de buen gobierno que deben cumplir los responsables públicos así como las consecuencias jurídicas derivadas de su incumplimiento -lo que se convierte en una exigencia de responsabilidad para todos los que desarrollan actividades de relevancia pública".

La Ley viene a fijar el régimen general del derecho de acceso a la información para todos los poderes públicos, atribuyendo a toda persona por igual la titularidad del derecho de acceso, cualquiera que sea su condición y sus circunstancias, y expresamente libera al solicitante de acceso de cualquier deber de motivar su petición de información. No es preciso ya que el ciudadano acredite un "interés legítimo" o directo en el conocimiento de la información que demanda. Pero al poder público si le impone el deber de motivar la negativa a hacer accesible la información solicitada por concurrir alguna de las limitaciones que prevé la Ley. Prima la transparencia y publicidad como regla general, salvo que prevalezca un interés, público o privado, del que derive un deber de reserva [311].

Uno de los aspectos más importantes es que intenta armonizar la normativa de protección de datos personales con la regulación de la transparencia de la actividad pública, estableciendo que su comunicación, por parte de los poderes públicos (sin consentimiento de su titular), estará restringido a un conjunto concreto de instituciones, por las importancia de las

[311] "La presente Ley tiene un triple alcance: incrementa y refuerza la transparencia en la actividad pública -que se articula a través de obligaciones de publicidad activa para todas las Administraciones y entidades públicas-, reconoce y garantiza el acceso a la información -regulado como un derecho de amplio ámbito subjetivo y objetivo- y establece las obligaciones de buen gobierno que deben cumplir los responsables públicos así como las consecuencias jurídicas derivadas de su incumplimiento -lo que se convierte en una exigencia de responsabilidad para todos los que desarrollan actividades de relevancia pública-. Este derecho solamente se verá limitado en aquellos casos en que así sea necesario por la propia naturaleza de la información-derivado de lo dispuesto en la Constitución Española- o por su entrada en conflicto con otros intereses protegidos. En todo caso, los límites previstos se aplicarán atendiendo a un test de daño (del interés que se salvaguarda con el límite) y de interés público en la divulgación (que en el caso concreto no prevalezca el interés público en la divulgación de la información) y de forma proporcionada y limitada por su objeto y finalidad.

funciones públicas que ejerzan y, para lo demás, limitado a los supuestos que expresamente autorice la Ley[312].

Una de las técnicas introducidas para la protección efectiva del derecho de acceso, es la atribución al silencio de la administración de un efecto positivo. Se trata de evitar las dilaciones en su ejercicio, por cuanto, en muchos casos, la información tiene fecha de caducidad que la hace inservible si no es actual.

El artículo 11, se refiere expresamente al derecho de acceso a la información pública y la protección de datos de carácter personal:

> "1. Cuando la solicitud de acceso se refiera a información pública que contenga datos de carácter personal se aplicarán las disposiciones previstas en esta Ley. No obstante, se aplicará la normativa de protección de datos personales cuando los datos que contenga la información se refieran únicamente al solicitante.
>
> 2. Si la información solicitada contuviera datos especialmente protegidos en los términos de la normativa de protección de datos personales, se denegará el acceso salvo que el titular de los datos consienta expresamente y por escrito su divulgación.
>
> 3. Con carácter general y, salvo que en el caso concreto prevalezca la protección de datos personales sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos vinculados con la organización, funcionamiento o actividad pública del órgano.
>
> 4. Asimismo, se podrá conceder el acceso a información que contenga datos personales que no tengan la consideración de

[312] Asimismo, dado que el acceso a la información puede afectar de forma directa a la protección de los datos personales, la Ley aclara la relación entre ambos derechos estableciendo los mecanismos de equilibrio necesarios. Así, por un lado, en la medida en que la información afecte directamente a la organización o actividad pública del órgano, prevalecerá la divulgación mientras que por otro se protegen-como no podría ser de otra manera- los datos que la normativa califica como especialmente protegidos, núcleo duro del derecho, para cuyo acceso se requerirá el consentimiento de su titular".

especialmente protegidos si, previa ponderación suficientemente razonada, el órgano competente para resolver considera que no se perjudica ningún derecho constitucionalmente protegido.

5. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los datos personales obtenidos a través del ejercicio del derecho de acceso".

JOSE LUIS PIÑAR MAÑAS, en su estudio sobre "Seguridad, Transparencia y Protección de Datos"[313], consideraba imprescindible conseguir un equilibrio entre estos conceptos, y señala que la protección de datos no puede considerarse un obstáculo al derecho de acceso a la información[314]. Para explicar su relevancia, acude a la jurisprudencia del TJCE, especialmente señala la sentencia del Tribunal de Justicia de 20 de mayo de 2003, Rundfunk[315] y otros, Asuntos C-465/00, C-138/01 y C-139/01, y la sentencia del Tribunal de Primera Instancia de 8 de noviembre de 2007, Bavarian Lager[316] contra Comisión, Asunto T-194/04, por cuanto

[313] PIÑAR MAÑAS, J.L., "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio". Documento de trabajo 147/2009. Laboratorio de Fundación Alternativas, Nº. 147. 2009. pp. 31-57

[314] SÁNCHEZ MORÓN, M. señala al respecto que (…) "algunas normas reconocen y regulan un derecho subjetivo de los particulares a requerir y obtener informaciones de las que disponen las Administraciones públicas y que no difunden de oficio (al menos, con carácter de información general al público). Dichas normas cumplen tres funciones complementarias en el ordenamiento jurídico. Primero, pretenden satisfacer el interés individual de los titulares del derecho a obtener una información que les puede afectar o que desean conocer, cualesquiera que sean las razones de su iniciativa. Desde este punto de vista, las normas que sancionan el acceso a la información contemplan un derecho subjetivo de carácter sustantivo, conectado con el derecho a recibir información veraz, aunque no se confunda con él. Sin embargo, este derecho, como casi todos, tiene también una dimensión objetiva, ya que repercute directamente sobre el modo de funcionamiento de la Administración, constriñéndola a aumentar su transparencia". SÁNCHEZ MORÓN, M. "El derecho de acceso a la información de medio ambiente". *Revista de Administración Pública*. Nº 137. Mayo-agosto 1995. p. 33. Disponible en: http://www.cepc.es/rap/Publicaciones/Revistas/1/1995_137_031.PDF

[315] PIÑAR MAÑAS, J.L., "Seguridad, transparencia…Op. Cit.: "La sentencia Rundfunk señala que en el tratamiento de datos personales son de aplicación los "principios relativos a la calidad de los datos" enunciados en el artículo 6 de la Directiva 95/46/CE y los "principios relativos a la legitimación del tratamiento de datos" enumerados en su artículo 7. En particular debe tenerse en cuenta el principio de finalidad y proporcionalidad, y el hecho de que según el citado artículo 7, letras c) y e), "el tratamiento de datos personales es lícito, respectivamente si, 'es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento', o si 'es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento [...] a quien se comuniquen los datos'" (apartados 65 y 66 de la sentencia).

[316] Ibídem: "La sentencia Bavarian Lager de 2007 juzga si era pertinente facilitar a terceros interesados los datos de las personas que intervinieron en una reunión de trabajo de la Comisión. El Tribunal parte de la base de que la lista de los participantes en la reunión que figuran en el acta de la misma contiene datos personales. Pero a partir de aquí lleva a cabo una serie de consideraciones que desembocan en la decisión de que tales datos deben ser facilitados cuando se lleva a cabo una solicitud de acceso a la información basándose en el Reglamento 1049/2001. Según el Tribunal, "debe constatarse que el mero hecho de que un documento contenga datos personales no significa necesariamente que se ponga en peligro la intimidad o la integridad de las personas de que se trata, a pesar de que la actividad

"sacan a la luz salen a la luz los principios esenciales del derecho a la protección de datos, en particular los de finalidad y proporcionalidad. Es en éstos donde debe encontrarse el equilibrio entre transparencia y protección de datos", pues el respecto a la protección de datos no siempre va a prevalecer, y habrá que analizar caso por caso, quedando en manos de los tribunales españoles determinar si hacer público o no el dato personal supondrá una vulneración de la Directiva 95/46/CE, ya que el proyecto de ley de transparencia no aporta soluciones concretas más allá de ponderar qué es interés público y si debe prevalecer sobre la naturaleza más o menos íntima del dato personal, tal y como se desprende de la redacción del artículo 11 arriba transcrito.

3.2.- Medidas de seguridad.

Como ya se ha señalado, en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea se reconoce el derecho a la protección de los datos de carácter personal y, "este derecho fundamental está contemplado en un marco jurídico europeo en materia de protección de los datos personales, en concreto, la Directiva 95/46/CE relativa a la protección de datos1, la Directiva 2002/58/CE sobre la privacidad y el Reglamento (CE) n° 45/2001 relativo a la protección de datos en el tratamiento por las instituciones y los organismos comunitarios. Esta normativa impone obligaciones a los responsables del tratamiento de datos y reconoce determinados derechos de las personas a quienes se refieren los datos. Asimismo, establece sanciones y medidas correctivas adecuadas en caso de infracción y contempla mecanismos de aplicación para garantizar su cumplimiento"[317].

profesional no esté, en principio, excluida del concepto de 'vida privada' en el sentido del artículo 8 del CEDH" (apartado 123 de la Sentencia).

[317] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET). Bruselas, 2.5.2007. COM (2007) 228 final.

Por otra parte, el Tribunal Constitucional, también reconoce en su Sentencia nº 254/1993, que "la llamada libertad informática es así el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".

El Habeas Data, entendido como instrumento de definición de garantía, constituye un cauce inicial para salvaguardar la libertad de la persona frente al uso de la informática y, que se caracteriza por la "acción"[318] procesal de protección de datos personales. Su objetivo es tan sólo cumplir una función paralela respecto de los derechos humanos de la tercera generación, la misma a que respondía el Habeas Corpus para los de primera generación, la liberta física o de movimientos de la persona, sin embargo, en el caso que nos ocupa es la garantía lo es para la libertad de decidir sobre la propia información personal.

El Habeas Corpus surgía como defensa frente a abusos de privación de la libertad física de la persona y, en la propia Exposición de Motivos[319] de la Ley Orgánica 6/1984, de 24 de mayo, Reguladora del Procedimiento "Habeas Corpus", se justifica su origen en nuestro sistema diciendo que "nuestra Constitución ha configurado, siguiendo esa línea, un Ordenamiento cuya pretensión máxima es la garantía de la libertad de los ciudadanos, y ello hasta el punto de que la libertad queda instituida, por obra de la propia Constitución, como un valor superior del Ordenamiento. De ahí que el texto constitucional regule con meticulosidad los derechos fundamentales, articulando unas técnicas jurídicas que posibilitan la eficaz salvaguarda de dichas derechos, tanto frente a los particulares como, muy especialmente, frente a los poderes públicos. Una de estas técnicas de protección de los

[318] Esta acción no existe todavía en España como "acción procesal" autónoma propiamente dicha, pero la idea de su consideración como tal es la que se quiere transmitir al citar este concepto. El individuo si puede accionar en España la actividad de los Tribunales para solicitar la defensa del derecho a la autodeterminación informativa.

[319] (...) "el constitucionalismo moderno tiene un objetivo fundamental, que constituye, al mismo tiempo, su raíz última: el reconocimiento y la protección de la vida y la libertad de los ciudadanos. Las constituciones que son verdaderamente tales se caracterizan, precisamente porque establecen un sistema jurídico y político que garantiza la libertad de los ciudadanos y porque suponen, por consiguiente, algo más que una mera racionalización de los centros de poder. Exposición de Motivos de la Ley Orgánica 6/1984, de 24 de mayo, Reguladora del Procedimiento "Habeas Corpus".

derechos fundamentales - del más fundamental de todos ellos: el derecho a la libertad personal - es la institución del Habeas Corpus"[320] (...), y tal y como se viene destacando, un aspecto no menos importante de la libertad, que requiere igualmente su propia técnica de protección, siguiendo la cadena de garantías de la libertad personal, es la autodeterminación informativa.

GIMENO SENDRA, atribuye al Habeas Corpus la naturaleza de derecho fundamental, por estar ubicado en la sección 1ª del Capítulo Segundo del Título I[321], sin embargo, y a pesar de su ubicación, su desarrollo normativo de la LO 6/1984, parece consolidarlo más bien como un instrumento de garantía procesal, derivado del derecho a la tutela judicial efectiva[322].

Al comparar el Habeas Corpus con un eventual Habeas Data, se puede observar que coinciden en lo referente a su naturaleza jurídica, porque en ambos casos se trata de instrumentos de garantía procesal de la libertad, física el primero e informática el segundo.

El término "Habeas Data" viene siendo utilizado, sobre todo en países latinoamericanos, para referirse a la normativa que protege los datos de carácter personal[323] y, en España, nos permite establecer paralelismos

---

[320] Continúa explicando, sobre su origen, que "Se trata, como es sabido, de un instituto propio del Derecho anglosajón, donde cuenta con una antiquísima tradición y se ha evidenciado como un sistema particularmente idóneo para resguardar la libertad personal frente a la eventual arbitrariedad de los agentes del poder público. Su origen anglosajón no puede ocultar, sin embargo, su raigambre en el Derecho histórico español, donde cuenta con antecedentes lejanos como el denominado recurso de manifestación de personas del Reino de Aragón y las referencias que sobre presuntos supuestos de detenciones ilegales se contienen en el Fuero de Vizcaya y otros ordenamientos forales, así como con antecedentes más próximos en las Constituciones de 1869 y 1876, que regulaban este procedimiento, aun cuando no le otorgaban denominación específica alguna".

[321] GIMENO SENDRA, V. *El proceso de Habeas Corpus.* Ed.Tecnos. Madrid, 1983. pp.44 y ss.

[322] Sentencia Tribunal Constitucional 44/1991, de 25 de Febrero. F.Jº. 2º: "Por lo que hace referencia a la pretendida vulneración del artículo 17.4, primera parte, C.E., es decir del derecho a la obtención del habeas corpus, ha de señalarse que el citado precepto constitucional no contiene propiamente un derecho fundamental sino una garantía institucional que resulta de la tutela judicial efectiva en todas sus vertientes". Un análisis de su regulación en el ordenamiento jurídico actual español, véase: GUIDE FERNÁNDEZ, A. *El Habeas Corpus en España*. Ed. Tirant Lo Blanch. Madrid, 2008.

[323] Ejemplos: La Constitución Brasileña de 1988, fue pionera en citar el "Habeas Data", en su artículo 5º bautizó constitucionalmente este instituto, adoptándolo como suyo de la Ley 824 del Estado de Río de Janeiro y, al señalar que se concederá Hábeas Data: "a) Para asegurar el conocimiento de informaciones relativas a la persona de quien lo pide, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) Para la rectificación de datos, cuando no se prefiera hacerlo en proceso reservado judicial o administrativo". Por otra parte, Uruguay: Ley Nº 17.838 de protección de datos personales para ser utilizados en informes comerciales y acción de Habeas Data (2004); Argentina: Ley Nº 25.326 - Ley de Protección de los datos personales (2000); Chile: Ley Nº 19.628 sobre Protección de la vida privada (1999); Perú: Ley Nº 27.489 que regula las centrales privadas de información de riesgos y de protección al titular de la información (2001), etc.

entre su finalidad y la del Habeas Corpus, para argumentar la necesidad de garantías de protección de la información personal. Así, por ejemplo, el derecho de acceso a la información personal de cada ciudadano, es asimilable a la obligación de la autoridad, en acto de la detención, de exhibir la orden escrita que lo dispuso, orden que en definitiva va a ser el instrumento que verdaderamente facilite al individuo el control sobre sus datos. En este sentido, otros ejemplos los constituyen el derecho a la información sobre el tratamiento de datos de carácter personal y, quién lo va a realizar, respecto del derecho de quien está siendo detenido, a que se le informe, en el mismo momento del hecho o de la causa que lo motiva; también la no obligación de declarar sobre la ideología, religión o creencias, y la previsión de que nadie puede ser obligado a declarar contra sí mismo.

En definitiva, la normativa sobre protección de datos personales no sirve de nada si no desarrolla garantías propias para su efectiva realización, y como ya se ha expuesto, estas garantías surgen con un haz de facultades de actuación personal (derechos), que trata de permitir al titular de los datos que de forma efectiva pueda decidir sobre el uso que de ello se vaya a hacer y, se apoyan en una serie de principios generales que han de guiar su ejercicio:

- Principio de Consentimiento[324]: el tratamiento de datos de carácter personal requiere (salvo en las excepciones previstas por Ley) el consentimiento del afectado, de carácter libre, inequívoco, específico e informado.
- Principio de Calidad: los datos de carácter personal sólo se podrán tratar cuando sean adecuados, pertinentes y no excesivos. Se mantendrán exactos y puestos al día o, en su caso, cancelados.
- Principio de Finalidad[325]: los datos no podrán ser utilizados para finalidades incompatibles con aquellas para las que hubieran sido recogidos debiendo haberse obtenido para finalidades determinadas, explícitas, y legítimas.

[324] Artículo 3. h) de la LO 15/1999 de Protección de Datos de Carácter Personal.
[325] Tanto el principio de calidad, como el de la finalidad se recogen en el artículo 4 de la LO 15/1999 de Protección de Datos de Carácter Personal.

- Principio de Información[326]: el afectado deberá ser informado de los extremos del tratamiento a que van a ser sometidos sus datos personales, de la identidad de quien lo va a realizar y de los derechos que sobre ello le asisten como titular.
- Principio de Seguridad de los Datos[327]: es necesaria la adopción de medidas de índole técnico y organizativo que garanticen la seguridad e integridad de los datos y eviten su alteración, pérdida o acceso no autorizado.

Pero todo ello, no tendría ningún sentido, si no cuenta con un marco jurídico bien definido, que incluya las obligaciones y responsabilidades de quienes vayan a tratar esos datos de carácter personal.

El Reglamento de Protección de Datos vigente[328] regula en nueve títulos el ámbito de aplicación y la definición de conceptos relativos a la realización práctica de las garantías que permiten la realización de la protección de datos. Y sin pretender un estudio pormenorizado de sus preceptos, ni de las novedades que introduce, nos detendremos en aquellas cuestiones que ponen de manifiesto un paso más en la evolución de esta materia y su aplicación práctica.

En el título I se contempla el objeto y ámbito de aplicación del reglamento, y da una serie de definiciones para el correcto entendimiento de la norma. El título II, se refiere a los principios de la protección de datos, especialmente lo que se refiere al modo de captación del consentimiento en supuestos muy específicos como son los servicios de comunicaciones electrónicas y, los datos de menores. El título III se ocupa de los derechos de las personas (acceso, rectificación, cancelación y oposición). Los títulos IV a VII señalan criterios específicos para el tratamiento de determinado tipo de ficheros de titularidad privada (relativos a la solvencia patrimonial y

[326] Artículo 5 de la LO 15/1999 de Protección de Datos de Carácter Personal.
[327] Artículo 10 de la LO 15/1999 de Protección de Datos de Carácter Personal. Las medidas que se deban adoptar dependerán del nivel de los datos que se vayan a tratar, y se estará a lo dispuesto por el Reglamento de Medidas de Seguridad, aprobado por Real Decreto 994/1999 de 11 de junio.
[328] El Reglamento sólo preveía una "vacatio legis" de 3 meses, entrando en vigor plenamente el día 19 de Abril de 2010, cumplidos todos los plazos transitorios.

crédito, y los utilizados en actividades de publicidad y prospección comercial) y, criterios específicos respecto a las obligaciones materiales y formales que deben seguir los responsables para la creación e inscripción de los ficheros, los procedimientos para la realización de transferencias internacionales de datos, y, los criterios que deben guiar la adopción de un "código tipo".

El principio de seguridad de datos del artículo 9 de la Ley Orgánica 15/1999, impone al responsable del fichero "adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. Y remite al desarrollo reglamentario el establecimiento de los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos". Y son los títulos VIII y IX del Reglamento los que contemplan en detalle la seguridad tecnológica, las "medidas de seguridad" que deben adoptar los responsables de un tratamiento de datos de carácter personal (o, en su caso, los encargados de un tratamiento), y que repercute sobre múltiples aspectos organizativos y de gestión.

Las medidas de seguridad se basan en los criterios de la confidencialidad o el acceso autorizado a los datos; la exactitud, o el impedir que la información sufra alteraciones no deseadas y, la disponibilidad, o la necesidad de que sólo las personas autorizadas puedan acceder a la información.

Son medidas de carácter técnico y organizativo que deben aplicarse a los ficheros de datos personales, entendidos como todo conjunto organizado y estructurado de datos de carácter personal, "cualquiera que fuere su forma o modalidad de creación, almacenamiento, organización y acceso. Se aplican a los centros de tratamiento, donde se encuentran los ordenadores, equipos y servidores que almacenan la información, y en ellos, a los lugares donde se encuentran físicamente ubicados los equipos y el

personal que trata datos", y a los equipos ("soporte físico que sirva para tratar y almacenar electrónicamente datos personales") y sistemas informáticos que tratan los datos de carácter personal. Asimismo, se aplicarán a las personas que tratan los datos, que "de acuerdo con sus funciones y obligaciones, interviene en cualquiera de las fases del tratamiento de los datos" (recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación, consulta, etc.).

Para ello, el Reglamento establece en el Capítulo III los niveles de seguridad aplicar para cada tipo de tratamiento, según el tipo de datos. El Nivel Básico, que se aplicará a todos los ficheros de datos de carácter personal; el Nivel Medio (que asumirá además las medidas de seguridad de nivel básico) que se adoptará para los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales; a la prestación de servicios de solvencia patrimonial y crédito; aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias; aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros; aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias; aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. Y el Nivel Alto (que asumirá además las medidas de seguridad de nivel básico y medio acumulativamente), que se aplicará a aquellos ficheros que contengan datos de ideología, religión, creencias, origen racial, salud, y vida sexual, los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual; los que contengan o se refieran a datos recabados para fines policiales sin

consentimiento de las personas afectadas; y aquéllos que contengan datos derivados de actos de violencia de género[329].

El articulado trata de ser particularmente minucioso en la fijación de las medidas y niveles de seguridad que corresponda adoptar, e instaura precauciones relativas al acceso a datos a través de redes de comunicaciones (artículo 85), al régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento (artículo 86), a los ficheros temporales o copias de trabajo de documentos (artículo 87), al propio documento de seguridad (artículo 88), a las funciones y obligaciones del personal (artículo 89), al imprescindible registro de incidencias (artículo 90), al control de acceso lógico y físico (artículo 91 y 99), a la gestión de soportes y documentos (artículo 92), a la identificación y autenticación de usuarios (artículo 93), a la realización de copias de respaldo y recuperación (artículo 94), a las auditorías (artículo 96), a la gestión de soportes y documentos (artículo 97), al almacenamiento de soportes no automatizados (artículo 107), su custodia (artículo 108), las copias o reproducciones (artículo 112), el acceso a la documentación (artículo 113), o su traslado (artículo 114).

Finalmente, el título IX, se dedica a los procedimientos tramitados por la Agencia Española de Protección de Datos.

Entre las novedades más destacadas del desarrollo aprobado en 2007, podemos señalar el artículo 2, apartados 2 y 3, con la aclaración del ámbito de aplicación de la normativa, diciendo que será de aplicación a "los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos

[329] Artículo 81. 4. "A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento. 5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando: a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. 6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos".

datos por los sectores público y privado, y excluye expresamente los tratamientos de datos referidos a personas jurídicas, los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales" y, los ficheros de datos relativos a "empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal"[330]. Matiza también, en el apartado cuarto, que el reglamento "no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos".

Llama la atención también que se haya delimitado con mayor precisión los conceptos de "dato personal" y "dato de salud":

- Datos de carácter personal: "Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".

- Datos de carácter personal relacionados con la salud: "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética".

[330] "El sujeto respecto del que pretenda llevarse a cabo el tratamiento es la empresa constituida por el comerciante industrial o naviero y no el empresario mismo que la hubiese constituido. Si la utilización de dichos datos se produjera en relación con un ámbito distinto quedaría plenamente sometida a las disposiciones de la Ley Orgánica". Informe de la AEPD 2008/0078.

Otra cuestión importante ha sido, tratar de definir qué es "interés legítimo" en el tratamiento de los datos[331]. El Reglamento regula de sistemáticamente las causas que determinan esa legitimidad, en particular, con previsiones específicas sobre el consentimiento tácito y la información que ha de facilitarse al interesado para el tratamiento de sus datos, pero el artículo 7 de la Directiva 95/46/CE señala: "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva". La legitimidad del tratamiento, va a afectar tanto al responsable como al encargado y va determinar en todo caso la aplicabilidad de las medidas de seguridad y la necesidad de preservar las garantías de ejercicio de derechos de los ciudadanos, de acuerdo con los principios básicos de la protección de datos.

Respecto del consentimiento del afectado, se reiteran las cualidades esenciales del mismo para que sea válido, que salvo excepciones legales, sea siempre y en todo caso, informado e inequívoco. Es decir, podrá ser tácito, pero el responsable tendrá la obligación de demostrar que existe y que ha sido debidamente informado. Asimismo, deberá esperar 30 días antes de proceder al tratamiento de los datos, a fin de conceder al interesado un plazo razonable para oponerse al tratamiento, y ello además, a través de un medio sencillo y que no suponga ingresos extra para el responsable del fichero. Una novedad en relación con el otorgamiento del consentimiento, es que se determina una edad mínima, en el artículo 13: "Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores".

[331] ÁLVAREZ RIGAUDIAS, C. "El Nuevo reglamento de desarrollo de la LOPD". *Actualidad Jurídica* Nº 21. Uría Menéndez. Año 2008. pp. 26.

En cuanto a las medidas de seguridad técnicas que se exigen para la custodia, almacenamiento y archivo de ficheros de datos personales, la principal novedad es sin duda la previsión de las especificaciones especiales para ficheros manuales (por ejemplo, puertas con llave)[332]. Otra cuestión novedosa es que se permita al responsable tener un solo Documento de Seguridad, o de tantos como ficheros existan, en función de la organización de la entidad. Siguiendo esta línea de control de los procedimientos, se precisa la "diligencia in eligendo" del responsable de seguridad, en la elección de un encargado de tratamiento de datos personales, que respete y cumpla la normativa tal y como la requiere el tratamiento que se encargue, con las condiciones de confidencialidad que sea necesario establecer al caso concreto.

En general, se puede decir que las novedades que el Reglamento vino a introducir en 2007, pretendían poner fin a las dudas y controversias más reiterativas, surgidas de la experiencia práctica de los tribunales y de la Agencia Española de Protección de Datos, sin embargo, la aprobación de estas nuevas reglas de juego produjo un nuevo debate sobre la importancia de la protección de datos, por cuanto surgían nuevas obligaciones para los responsables y encargados de los tratamientos de datos, y se planteaban nuevos retos para la resolución de controversias en esta materia[333]. Así, el Real Decreto 1720/2007 fue impugnado nada más nacer por distintas entidades que jugaban dicho papel, la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)[334], la Federación de

[332] Artículo 105 y siguientes. ACED FÉLEZ, E. Subdirector General de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid. Ponencia "Novedades del Reglamento de desarrollo de la LOPD". VI Jornada de Protección 2 de Datos Sanitarios – Madrid, 23 de abril de 2008.

[333] "El derecho fundamental a la protección de datos personales. Contenidos esencial y retos actuales. En torno al nuevo Reglamento de Protección de datos". Estudio Introductorio. *Legislación de Protección de Datos.* PIÑAR MAÑAS, J.L. y CANALES GIL, A. Ed. Iustel. Madrid, 2008. p.90.

[334] Solicitando que "se declarase la nulidad de los siguientes preceptos del Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre: Artículo 5. Definiciones. Del apartado 1.q), el inciso "aunque no lo realizase materialmente". Artículo 8. Principios relativos a la calidad de los datos, en el párrafo 3º de su apartado 5. Artículo 10. supuestos que legitiman el tratamiento o cesión de los datos, en los apartados 2.a), supuesto primero, y 2.b), párrafo primero. Artículo 11. Verificación de datos en solicitudes formuladas a las Administraciones Públicas. Artículo 12. Principios generales, en su apartado 2. Artículo 13. Consentimiento para el tratamiento de datos de menores de edad, en su apartado 4. Artículo 18. Acreditación del cumplimiento del deber de información. En el inciso final de su apartado 1 y en su apartado 2. Artículo 21. Posibilidad de subcontratación de los servicios. En su apartado 2.a). Artículo 23. Carácter personalísimo, en su apartado 2.c). Artículo 24. Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, el inciso final del párrafo 1º del artículo 24.3 y el párrafo 2º del mismo artículo. Enunciado de la Sección 2ª, del Capítulo I del Título IV, en cuanto se refiere también al "cumplimiento" de obligaciones dinerarias. Artículo 38. Requisitos para la

Comercio Electrónico y Marketing Directo[335], y por Experian Bureau de Crédito, S.A[336], por considerar parte de su articulado contrario al derecho comunitario y al derecho interno[337], resolviéndose las cuestiones principales por las Sentencias del Tribunal Supremo nº 23/2008; nº 25/2008 y, nº 26/2008, todas ellas de 15 de Febrero 2010, dictadas por la Sala de lo Contencioso-Administrativo, Sección Sexta.

El Tribunal Supremo, a través estas sentencias decidió declarar nulos una serie de artículos y seccionar parte de otros, atendiendo las peticiones de los demandantes.

En la primera de las Sentencias (23/2008); el Tribunal Supremo decide desestimar la solicitud inicial de nulidad del Reglamento en su totalidad; decide dejar imprejuzgada la "impugnación del artículo 10.2. a) y b), por planteamiento de cuestión prejudicial ante el Tribunal de Justicia de

---

inclusión de los datos, en sus apartados 1.a) (en el inciso "y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero") y b) (en el inciso "o del plazo concreto si aquélla fuera de vencimiento periódico"), 2 y 3. Artículo 39. Información previa a la inclusión, en el inciso "en el momento en que se celebre el contrato". Artículo 40. Notificación de inclusión, en su apartado 2. Artículo 41. Conservación de los datos, en el párrafo segundo del apartado 1 y en el apartado 2 (en el inciso <<o del plazo concreto si aquélla fuera de vencimiento periódico"). Artículo 42. Acceso a la información contenida en el fichero, en su apartado 2, inciso "por escrito" del párrafo primero y todo el párrafo segundo. Artículo 44. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición, en su apartado 3, 1ª, en el inciso "en el plazo de siete días". Artículo 45. Datos susceptibles de tratamiento e información. En el inciso "habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad", del apartado 1.b). Artículo 46. Tratamiento de datos en campañas publicitarias. En las letras b) y c) del apartado 2, y en todo su apartado 3. Artículo 47. Depuración de datos personales. Artículo 49. Ficheros comunes de exclusión del envío de comunicaciones comerciales. En sus apartados 2 y 4.Artículo 69. Suspensión temporal de las transferencias, en su apartado 1.b) (inciso "o no van a adoptar en el futuro"). Artículo 70. Transferencias sujetas a autorización del Director de la Agencia Española de Protección de datos, en su apartado 3. letras c) (inciso "o no serán respetadas"), d (inciso "o no serán") y d). Artículo 123. Personal competente para la realización de las actuaciones previas, en su apartado 2, inciso "o a funcionarios que no presten sus funciones en la Agencia".

[335] Solicitando se declarase la nulidad de los artículos: "Artículo 5.1 q) in fine; Artículo 49; Artículo 47; Artículo 12.1, segundo párrafo; Artículo 8.5; Artículo 18; Artículo 20.1; Artículo 10 apartados 2 a) y 2 b); Artículo 45.1 b) in fine; Artículo 46, apartados 2,3 y 4; Artículo 13.4; Artículo 42; Artículo 38, apartado 1a) (la frase "y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero"), y apartado 1 b), y Artículos 38.2 y 38.3".

[336] Solicitando se declarase la nulidad de los artículos: "El inciso "cumplimiento o" en la rúbrica de la Sección 2ª del Capítulo I del Título IV; el inciso "cumplimiento o" en el artículo 39; el inciso "o administrativa, o tratándose de servicios financieros, se haya planteado una reclamación en los términos previstos en el Reglamento aprobado por el Real Decreto 303/2004, de 20 de febrero" en el artículo 38.1 a); el artículo 41.1, párrafo segundo; el inciso "por escrito" del párrafo primero del artículo 42.2, y todo el párrafo segundo del artículo 42.2".

[337] El Tratado Constitutivo de la Comunidad Europea; la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31); y a la Ley Orgánica 15/1999, por cuanto transpone al derecho español dicha norma.

las Comunidades Europeas, y hasta que dicho Tribunal se pronuncie sobre la cuestión de mención, y decide anular, por disconformes a derecho, los artículos 11[338], 18[339], 38. 2[340], y 123.2[341] de la disposición reglamentaria, así como la frase del artículo 38.1.a) que dice así: "... y al respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero".

Para mostrar las razones jurídicas alegadas para determinar la nulidad de los diferentes artículos, se ha analizado la primera de las Sentencias por considerarse la más completa. En ella, para anular el artículo 11, se justifica que implicaba un tratamiento o cesión de datos no consentido ni habilitado legalmente, según lo dispuesto por los artículos 6 y 11 de la Ley Orgánica 15/1999, relativos precisamente al consentimiento del afectado y a la comunicación de datos. Para anular el artículo 18, se alega que imponía una obligación de constancia documental que excede lo dispuesto por el artículo 5 de la LOPD, que prevé libertad formal en la

[338] Artículo 11. "Verificación de datos en solicitudes formuladas a las Administraciones públicas. Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la autenticidad de los datos".

[339] DEBER DE INFORMACIÓN AL INTERESADO (secc. 2ª): Artículo 18. "Acreditación del cumplimiento del deber de información. 1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado. 2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales".

[340] Artículo 38. "Requisitos para la inclusión de los datos. 2. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores. Tal circunstancia determinará asimismo la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero".

[341] Artículo 123. Personal competente para la realización de las actuaciones previas. "2. En supuestos excepcionales, el Director de la Agencia Española de Protección de Datos podrá designar para la realización de actuaciones específicas a funcionarios de la propia Agencia no habilitados con carácter general para el ejercicio de funciones inspectoras o a funcionarios que no presten sus funciones en la Agencia, siempre que reúnan las condiciones de idoneidad y especialización necesarias para la realización de tales actuaciones. En estos casos, la autorización indicará expresamente la identificación del funcionario y las concretas actuaciones previas de inspección a realizar. Los funcionarios que ejerzan la inspección a los que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos. Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas".

recogida del consentimiento (verbal o escrito). Para anular el referido párrafo del artículo 38.1.a, se alega que presenta una redacción defectuosa, y se reconoce que "la aplicación de la norma puede producir efectos adversos al permitir evitar la inclusión del dato relativo a la deuda en los ficheros de solvencia patrimonial, y reconoce también que esos efectos adversos es posible contemplarlos cuando se incluye en un fichero de esa naturaleza la existencia de una deuda inexistente, no vencida o inexigible"[342]. Para anular el artículo 38. 2, se alega que la prueba indiciaria no "es una prueba admitida en nuestro derecho, pero no lo es menos, y valga al respecto la cita de la sentencia de la Sala de lo Civil de este Tribunal de 16 de septiembre de 1996, que no es equiparable a la prueba de presunciones. Sin duda juega un papel relevante en el ámbito cautelar, pero ha de reconocerse que la redacción de la norma al no concretar qué principio de prueba exige (documental, pericial, testifical, etc.), junto a la dificultad de apreciación del grado exigible de la prueba indiciaria, origina en efecto una inseguridad jurídica que debe corregirse". Y por último, para anular el artículo 123. 2, se alega que se trata de una cuestión que afecta directamente a las capacidades de contratación del Director de la Agencia, y que le concede una nueva, que no está prevista en los artículos 35, 37 o 40 de la LOPD[343].

La segunda de las Sentencias (25/2008), siguiendo lo dispuesto en la anterior, el Tribunal Supremo decide desestimar la solicitud inicial de nulidad del Reglamento en su totalidad, mantiene su decisión de dejar imprejuzgada la "impugnación del artículo 10.2. a) y b), por el

[342] F. Jº 14 Sentencia 23/2008 TS: "No otra cosa puede decirse si nos atenemos a lo dispuesto en el artículo 6.1.d) de la Directiva que exige que los datos sean exactos y, cuando sea necesario, actualizados, así como que se tomen todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueran recogidos o para los que fueron tratados posteriormente, sean suprimidos o ratificados, pues mal puede entenderse que unos datos no son exactos y no se encuentran actualizados como consecuencia de una reclamación de cualquier naturaleza en instancias judiciales, arbitrales, administrativas o ante los Comisionados".

[343] Ibídem. F. Jº 22: "El artículo 35.3 hace mención a que los puestos de trabajo de los órganos y servicios que integren la Agencia serán desempeñados por personal funcionario o contratado; el artículo 36, también del Texto Legal, relativo a la naturaleza y funciones del Director de la Agencia, no incluye la designación que contempla el artículo 123.2, y lo mismo sucede con el artículo 37, en el que se enumeran las funciones de la Agencia. Tampoco el artículo 40, que, relativo a la potestad de inspección, prevé en su apartado 2 que "Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos" y que "Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas". A excepción de los preceptos legales referenciados ningún otro de la Ley hace mención al personal que ha de ocupar los puestos de trabajo de los órganos y servicios que integren la Agencia".

planteamiento de la cuestión prejudicial ante el Tribunal de Justicia de las Comunidades Europeas y, mantiene la decisión de anular, por disconforme a derecho, el artículo 18 de la disposición reglamentaria".

En la tercera de las Sentencias (26/2008), siguiendo lo dispuesto en la anterior, el Tribunal Supremo decide anular, "por disconforme a derecho, Anular por disconforme a derecho la frase del artículo 38.1.a): "(...) o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de los servicios financieros aprobado por Real Decreto 303/2004, de 20 de febrero". Quedaría este apartado con la siguiente redacción, al aplicar ahora esta ampliación a la nulidad del apartado, respecto de lo señalado por la primera sentencia: "38. 1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos: a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada".

En conclusión, los preceptos afectados no forman hoy parte del régimen legal de la protección de datos, independientemente de que otros puedan resultar igualmente anulados, a la luz de la respuesta que ofrezca en su momento el TJUE a las cuestiones prejudiciales planteadas[344] y, la definición del "interés legítimo", podría venir directamente impuesta por el artículo 7.f de la Directiva 95/46/CE.

[344] En concreto, la impugnación del artículo 10.2. a) y b), que después de permitir el tratamiento y la cesión de los datos de carácter personal si el interesado presta previamente su consentimiento (apartado 1), dispone en el apartado 2: "No obstante, será posible el tratamiento o la cesión de datos de carácter personal sin necesidad del consentimiento del interesado cuando: a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes: El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre. El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas. b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tengan un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado. No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello con una norma con rango de ley".

3.3.- Tecnologías para la protección (PET).

Una vez analizada la previsión constitucional, el concepto y, la garantía procesal, procede en este apartado considerar la parte de la práctica que tiene la responsabilidad de hacer efectivo lo anterior: la tecnología, los derechos de los ciudadanos y las medidas de seguridad.

La Comisión Europea ha elaboró en este sentido, en Mayo de 2007, la "Comunicación de la Comisión al Parlamento Europeo y al Consejo, sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad" (PET[345]). Este informe, pretendía poner de relieve que, tanto las ventajas como los inconvenientes de la tecnología deben ser considerados para una correcta protección de los individuos cuya información circula por los sistemas informáticos.

La propia Directiva 2002/58/EC contempla en cierta forma[346] el uso de la tecnología para favorecer el cumplimiento de la legislación relativa a la protección de datos y, estas tecnologías son las denominadas "tecnologías de protección de la intimidad" (PET), que deben contribuir a minimizar el tratamiento de datos personales y al empleo de datos anónimos o seudónimos siempre que sea posible, dificultando la vulneración de los derechos del ciudadano también desde el punto de vista técnico y, con su informe, "la Comisión quiere fomentar dichas tecnologías y definir medidas claras para conseguirlo favoreciendo el desarrollo de las PET y su utilización por parte de los responsables del tratamiento de datos y los consumidores".

Es evidente que hablar de tratamientos informáticos y procesos automatizados con datos de carácter personal, exige poner en relación directa las medidas de seguridad con que la legislación pretende dar sentido a la garantía que de sus preceptos sobre esta materia, de tal forma que se tienda a tratamientos estrictamente necesarios y con mínimo riesgo o

[345] *Privacy Enhancement Techniques* (Tecnologías de Mejora de la Privacidad).
[346] Considerando 46 y artículo 14, apartado 3.

impacto sobre la dignidad y los derechos de las personas afectadas. La Comisión expone en su informe varios ejemplos de lo que implican las PET:

> • "La anonimización automática de los datos tras un lapso de tiempo determinado obedece al principio de que los datos tratados deben guardarse en una forma que permita identificar al interesado únicamente durante el tiempo necesario para los fines iniciales para los cuales se facilitan los datos.
>
> • Los instrumentos de cifrado que impiden el pirateo de la información transmitida por Internet responden a la obligación del responsable del tratamiento de datos de adoptar medidas adecuadas para proteger los datos personales frente al tratamiento ilícito.
>
> • Los anuladores de cookies, que bloquean las cookies introducidas en un ordenador para que lleve a cabo determinadas instrucciones sin que el usuario tenga conocimiento de ello, responden al principio de que los datos deben tratarse de forma lícita y transparente y que ha de informarse al interesado del tratamiento que se realice.
>
> • La Plataforma de Preferencias de Privacidad (P3P), que permite a los usuarios de Internet analizar la política de los sitios web por lo que se refiere a la intimidad y compararla con las preferencias del usuario en relación con la información que desee facilitar, contribuye a garantizar que el interesado autoriza el tratamiento de sus datos con conocimiento de causa".

Son estos ejemplos la expresión práctica de la normativa de protección de datos. Cómo se puede adaptar el progreso a las necesidades del tratamiento de información personal sin lesionar, o con mínimo riesgo, el derecho de los individuos a decidir sobre la información que le concierne.

Permiten en definitiva evitar las infracciones de la normativa en materia de protección de datos e, indirectamente, de otras materias como lo relativo al derecho a la intimidad. Más aún, como señala la propia Comisión, las PET también "podrían favorecer la protección de intereses públicos importantes. Con arreglo al marco jurídico de la protección de datos personales, la aplicación de los principios generales y el respeto de los derechos de los ciudadanos pueden limitarse para preservar intereses públicos importantes, como la seguridad pública, la lucha contra la delincuencia o la salud pública".

Y, para que todo esto configure la protección que se pretende, la Comisión plantea sus objetivos con acciones a desarrollar en este ámbito, en las que incluye la participación de las autoridades nacionales, el sector empresarial y los consumidores.

El primer objetivo es "respaldar el desarrollo de las PET", de forma que su diseño, elaboración y puesta en el mercado se haga bajo una serie de normas de calidad que puedan avalar su funcionamiento conforme a la finalidad para la que hayan sido creadas. Para ello prevé dos acciones fundamentales, la primera: determinar la necesidad de PET y los requisitos tecnológicos que precisen para hacer frente a los peligros que se planteen en relación con los derechos fundamentales. La segunda, respecto del desarrollo de las PET, es decir, acciones dirigidas a adoptar medidas concretas para lograr un resultado concreto, "un producto final listo para el uso" que se le haya asignado[347].

Otro objetivo es alentar a los responsables del tratamiento de datos a emplear las PET disponibles. En este empeño, la Comisión trata de concienciar a los encargados de realizar los tratamiento y sus responsables,

[347] La Comisión ya lo está haciendo: "dentro del Sexto Programa Marco, patrocina el proyecto PRIME (https://www.prime-project.eu/), que hace frente a los problemas relacionados con la gestión de la identidad electrónica y la protección de la intimidad en la sociedad de la información. El proyecto OPEN-TC (http://www.opentc.net/) permitirá proteger la intimidad mediante sistemas informáticos abiertos fiables y el proyecto DISCREET (http://www.ist-discreet.org/) desarrolla middleware para proteger la intimidad en los servicios de red avanzados. En el futuro, dentro del Séptimo Programa Marco, la Comisión tiene previsto financiar otros proyectos de IDT y demostraciones piloto a gran escala para desarrollar y favorecer la incorporación de las PET. El objetivo consiste en sentar las bases de unos sistemas de protección de la intimidad que responsabilicen al usuario y superen las disparidades jurídicas y técnicas observadas en Europa mediante asociaciones entre el sector público y el privado".

del hecho de que, incorporar efectivamente las PET al uso habitual de los equipos técnicos y lógicos con que se realizan los tratamientos de datos personales, es estrictamente necesario para cumplir la normativa y evitar no sólo las indeseadas lesiones de derechos fundamentales, sino también como las graves sanciones que ello conlleva. En este sentido, las acciones propuestas por la Comisión Europea se dirigen principalmente a fomentar el uso de las PET en beneficio de todos los agentes que participan en el tratamiento de datos personales y, en el respeto de normas relativas a la protección de la información personal mediante PET, dictadas por las diferentes legislaciones nacionales[348], que obliguen a todos los agentes intervinientes en los tratamientos, incluidas las Administraciones Públicas. Éstas, en especial, deben observar con estricta diligencia el uso que hacen de la tecnología en relación con el tratamiento de datos personales, bien por el volumen de información que tratan, bien por el alcance que conllevan sus decisiones y sus operaciones (derivadas precisamente del tratamiento de información personal) respecto de los administrados, tal como se menciona en la Comunicación de la Comisión sobre el papel de la administración electrónica en el futuro de Europa[349], "la administración electrónica debe emplear PET con objeto de generar la confianza necesaria para funcionar de forma satisfactoria. La Comisión invita a los Gobiernos a que garanticen la protección de datos en los programas de administración electrónica, entre otras cosas recurriendo en la mayor medida posible a las PET en el diseño y aplicación de los mismos".

Por último, el tercer objetivo que se plantea la Comisión en su Informe, es el de alentar a los consumidores para que utilicen las PET, pues no en vano son los principales interesados en que, la información que sobre ellos manejan empresas y administraciones, sea tratada con las debidas garantías de seguridad. Sin embargo, este propósito, no se dirige tanto a la

[348] "El Grupo de Trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la Directiva 95/46/CE, que persigue la aplicación uniforme de las medidas nacionales adoptadas conforme a la Directiva, podría contribuir a ello. Así pues, la Comisión invita a dicho Grupo de Trabajo a que prosiga su labor en ese ámbito incluyendo en su programa una actividad permanente de análisis de las necesidades relativas a la incorporación de PET en las operaciones de tratamiento de datos como medio eficaz para garantizar el respeto de las normas de protección de datos. Esa labor debería plasmarse en unas directrices que las autoridades de protección de datos personales aplicarían a nivel nacional gracias a la adopción coordinada de los instrumentos pertinentes".

[349] COM (2003) 567 final, de 26.9.2003.

parte técnica de las PET como a la parte práctica, es decir, exige que exista un conocimiento práctico por los consumidores sobre las herramientas a su alcance para la protección de sus derechos fundamentales y, de los riesgos que pueden derivarse de un uso negligente de las mismas. Así, se trataría de sensibilizar a los consumidores, con una información sencilla y comprensible y, de facilitarles la elección entre los diferentes sistemas de protección a su alcance. A tal efecto, la Comisión prevé la posibilidad de instaurar un sistema europeo de distintivos de protección de la privacidad. Gracias a esto distintivos, "los consumidores podrían reconocer fácilmente los productos que cumplen o favorecen el cumplimiento de las normas de protección de datos en el tratamiento de éstos, en concreto mediante la aplicación de PET apropiadas" y, para lo cual sería deseable que se observaran los siguientes principios:

- "El número de sistemas de distintivos debería reducirse al mínimo, pues la proliferación de distintivos podría crear mayor confusión al consumidor y mermar su confianza en todos los distintivos; de ahí la pertinencia de valorar si sería preciso integrar —y en qué medida— un distintivo europeo de protección de la intimidad en un sistema más general de certificación de seguridad[350].

- Los distintivos deberían concederse únicamente a los productos que cumplan una serie de reglas que corresponden a las normas de protección de datos. Las reglas deberían ser tan uniformes como fuera posible en toda la UE.

- Las autoridades públicas, en particular las autoridades nacionales responsables de la protección de datos personales, deberían desempeñar un papel importante en el sistema participando en la definición de reglas y procedimientos

[350] En su Comunicación de 31 de mayo de 2006, titulada "Una estrategia para una sociedad de la información segura: Diálogo, asociación y potenciación" [COM (251) final], la Comisión invita al sector privado a "trabajar en favor de unos regímenes de certificación de la seguridad aplicables a productos, procesos y servicios que sean asequibles y respondan a las necesidades específicas de la UE (en particular, en relación con la privacidad)".

pertinentes, y en la supervisión del funcionamiento del mismo".

Teniendo en cuenta lo expuesto, la labor que pretende la Comisión desde mediados del año 2007, significa que, además de aplicar su experiencia previa en programas de distintivos en otros ámbitos (medio ambiente, agricultura, certificación de seguridad para productos y servicios, etc.), exige mantener un diálogo fluido con todas las partes afectadas, incluidas las autoridades nacionales responsables de la protección de datos, las asociaciones empresariales y de consumidores y los organismos de normalización, y todo ello con la finalidad última de incentivar el uso de tecnologías fiables y seguras en los tratamientos de datos personales en el marco de la Unión Europea.

3.4.- Identificador único.

La utilización de la tecnología, para el tratamiento de datos personales, sin las debidas garantías, implicaría un atentado directo contra los pilares de toda sociedad democrática. La propia CE enumera entre los fundamentos de orden público y paz social, la dignidad de la persona y el libre desarrollo de su personalidad, porque el ciudadano debe ser el protagonista de la vida democrática, y porque las decisiones de los poderes públicos deben estar orientadas a que su libertad y dignidad queden protegidas de otros intereses menos relevantes.

El aumento ilimitado del control estatal, sin normas, derechos, o tecnologías de protección de los ciudadanos que eviten el desvío de su información hacia fines no autorizados, debilitaría el Estado de Derecho hasta convertirlo en el totalitarismo más absoluto, presidido por pautas de

vigilancia individualizada e identificada, a través de un cerco informático opresor al servicio del gobierno[351].

En este sentido, asignar un código identificador universal a cada ciudadano, que permite reunir e interrelacionar todos los datos existentes en los ficheros públicos, y en muchos del sector privado, sin las debidas garantías, sería el supuesto más peligroso y más cercano al "gran hermano" de Orwell, pues dejaría en manos del Estado la opción de cotejar todo tipo de datos informatizados, accediendo a auténticos perfiles de cada uno de los individuos que gobierna[352].

Explica MARTÍN PALLÍN que "detrás de la utilización de los números como signo de identidad existe un número totalitario. Se comprende la tentación de abandonarse a la comodidad de sus usos, pero cualquier persona sensible y con espíritu democrático debe rechazar de inmediato este primer impulso y meditar seriamente sobre las consecuencias negativas y antidemocráticas que acarrea la implantación del sistema. La imagen del hombre de cristal, que utilizamos frecuentemente los que nos preocupamos por estos temas, aparece como una realidad tangible". Y que el control alcanza cotas máximas, si se acude a procedimientos de identificación numérica de los ciudadanos y, el sistema agiliza al máximo la difusión de información. "La personalidad se difumina y el control se vuelve asfixiante cuando el ciudadano pasa a ser un número, que introducido en un sistema informático deja a un lado su nombre, circunstancias y lazos vitales. La uniformidad identificadora puede convertirse en un lazo inmovilizador que maniate cualquier capacidad de autodeterminación"[353].

---

[351] (…) "las autoridades administrativas a través de simples normas reglamentarias no sometidas a límites precisos e inequívocos, pueden organizar un tráfico intenso de datos personales entre sus ficheros que, en última instancia, equivaldría al "gran fichero único" dónde se centralizasen todos los datos de los ciudadanos" (...). CARRASCOSA, V. "La protección de los datos personales". Regulación nacional e internacional de la seguridad informática. Generalitat de Cataluña. Barcelona, 1993. pp. 209-210.

[352] La Constitución portuguesa de 1976, prohíbe en su artículo 35. 3 atribuir un número nacional único a los ciudadanos.

[353] MARTÍN PALLÍN, J.A. "Constitucionalidad del número identificador único". *Jornadas sobre el derecho español de la protección de datos*. Agencia de Protección de Datos. 28, 29 y 30 de Octubre de 1996. Madrid. pp. 61 y 66.

Un número de identidad universal, puede facilitar la fluidez de las cesiones de datos, y de su interrelación, proporcionando sin límites todo tipo de informaciones, pudiendo afectar a la dignidad del ciudadano, al ser tratado como una cifra que le persigue de por vida, y que participará de todo tipo de valoraciones que el Estado quiera hacer sobre cuál es su papel en la sociedad. Y precisamente por la importancia que adquieren las garantías constitucionales ante un supuesto como el identificador universal, merece consideración aparte la generalización de su uso.

El contenido del Documento Nacional de Identidad[354], el dato en sí, no es excesivo para los fines de "identificar" al sujeto ciudadano como tal, y además, no afecta a su esfera privada o íntima, pues en principio no revela este tipo de informaciones. Consigna datos personales como la fotografía, la huella digital o el domicilio, y en España es obligatorio, a partir de los 14 años, el D.N.I., a los únicos fines de identificación ciudadana, pero hasta hace relativamente poco, no era necesario que su adopción nos pusiese en relación directa con otras finalidades como la identificación como conductor de vehículos a motor (permiso de conducir) o, el tratamiento de datos fiscales.

La consagración del sistema identificador único, se produjo con la instauración del Número de Identificación Fiscal (N.I.F), en el artículo 113 de la Ley 33/1987, de 23 de diciembre de Presupuestos Generales del Estado para 1988, desarrollada por el Real Decreto 338/1990, de 9 de marzo, por el que se regula la composición y la forma de utilización del Número de Identificación Fiscal[355] y la Orden Ministerial de 14 de marzo de 1990.

Esta normativa, fue impugnada por el Consejo General de Colegios de Economistas, que interpuso recurso contencioso-administrativo contra el Real Decreto 338/1990, de 9 de marzo, y la Orden Ministerial de 14 de

[354] Decreto 196/1976, de 6 de febrero, por el que se regula el Documento Nacional de Identidad. Aunque es la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, en su artículo 9, reconoce el derecho de todos los españoles a que se les expida el Documento Nacional de Identidad, al que se atribuye el valor suficiente para acreditar, por sí solo, la identidad de las personas y le otorga la protección que a los documentos públicos y oficiales es reconocida por el ordenamiento jurídico.
[355] BOE Nº 63, de 14 de marzo de 1990.

marzo de 1990, por considerar que en la regulación de la composición y la forma de utilización del Número de Identificación Fiscal (NIF), vulneraban el derecho fundamental a la intimidad consagrado en el artículo 18 CE, y que adolecían de defectos procedimentales y formales que acarreaban su nulidad de pleno Derecho.

La Sentencia del Tribunal Constitucional nº 143/1994, de 9 de mayo de 1994, centra su argumentación en determinar si la transmisión de informaciones sobre actividades desenvueltas en el tráfico económico negocial, vulnera o no el derecho a la intimidad personal. El derecho a la intimidad garantiza un ámbito propio y reservado frente a la acción y el conocimiento de los demás[356], y por eso, señala el TC, resulta difícil que pueda resultar afectado por el hecho de tener que facilitar información económica y, en cualquier caso, recuerda, que este derecho no es absoluto.

El Tribunal considera que no vulnera el artículo 18 de la CE, porque al recoger las garantías precisas para que ello no ocurra, se respeta el mandato constitucional. En particular señala que el identificador único universal, tal y como está regulado, en El Real Decreto 338/1990, lo mismo que su orden de desarrollo, "forman parte de un conjunto normativo que introduce garantías suficientes frente al eventual uso desviado de la información que aquellas normas permiten recabar. En este marco destaca, en desarrollo del artículo 18.4 CE, la Ley Orgánica de 29 de octubre de 1992, de regulación del tratamiento automatizado de los datos de carácter personal, que aparte, de las reglas generales sobre tratamiento de datos que no vienen ahora al caso, establece normas específicas para restringir el

[356] (F.Jº. 7º) (...) "Como ya se ha anticipado, cuestiona la demanda la legitimidad constitucional de una norma que, a través de un instrumento de recopilación de información, puede propiciar un uso desviado de ésta y, en consecuencia, la efectiva invasión de la esfera privada de los ciudadanos afectados. Desde luego, es un hecho también admitido en la jurisprudencia de este Tribunal que el incremento de medios técnicos de tratamiento de la información puede ocasionar este efecto y, correlativamente, se hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto, que produzca este efecto, y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho [STC 254/1993]. En este sentido se ha afirmado que, ya que "los datos personales que almacena la Administración son utilizados por sus autoridades y servicios", no es posible "aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión" (STC 254/1993, F.Jº. 7º). En consecuencia con ello, habría que convenir en que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta".

defecto que la parte imputa a la norma reglamentaria impugnada. En concreto, garantizándose la seguridad de los archivos (artículo 9), imponiéndose un deber específico de secreto profesional, incluso después de finalizadas sus tareas al respecto, al «responsable del fichero automatizado y (a) quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal» (artículo 10) e impidiendo la transmisión de datos de carácter personal almacenados, con la excepción de que concurra el consentimiento del interesado, la autorización legal específica o la conexión y reconocida necesidad de la transmisión de datos para el logro de finalidades constitucionalmente relevantes (artículo 11) en las condiciones dispuestas en la norma. Todas ellas como garantías para determinar el carácter proporcionado y razonable de la obligación de transmitir información fiscal puesto de manifiesto en la doctrina de este Tribunal (STC 110/1984, F.Jº. 4º)"[357].

Por último, en materia de peligros y garantías precisas para evitarlos, es necesario hacer referencia expresa al DNI electrónico[358], por cuanto en él tomarían especial relevancia los riesgos de una hipotética falta de garantías y límites, frente a la voraz vocación controladora de las Administraciones Públicas. Valiéndose de todo tipo de tecnologías, con el tratamiento del DNI electrónico, se podrían producir sin demasiadas dificultades una sociedad de "ciudadanos de cristal", accediendo a toda la información personal que se haya querido (o se haya obligado) almacenar en la memoria del circuito integrado (chip) que integra el DNI electrónico, y utilizándola para cualesquiera otros fines que no sean los propios de la normativa que le da vida[359].

La Ley 59/2003, de 19 de diciembre, de firma electrónica, atribuyó al Documento Nacional de Identidad nuevos efectos y utilidades, como son los de poder acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y

[357] Ibidem.
[358] http://www.dnielectronico.es Web de información acerca del DNI-e, de la Dirección General de la Policía y de la Guardia Civil.
[359] La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. DOCE N° L 013 DE 19/01/2000. pp. 0012-0020.

la integridad de los documentos firmados con los dispositivos de firma electrónica, incorporada al mismo. Y el desarrollo de esas funciones[360], se produjo con el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula documento nacional de identidad y sus certificados de firma electrónica[361], modificado en el año 2009[362].

Entre las supuestas ventajas de llevar almacenada electrónicamente nuestra información personal, se señalan las posibilidades de realizar transacciones con entidades bancarias y compras seguras a través de Internet, hacer trámites completos con las Administraciones Públicas a cualquier hora, acceder a determinados edificios públicos, o utilizar de forma segura nuestro ordenador personal, por ejemplo, al participar en un conversación por Internet, para tener la certeza de que nuestro interlocutor es quien dice ser. Asimismo, e independientemente del cumplimiento de la LOPD y de las medidas de seguridad del Reglamento de desarrollo, por aquellas entidades con las que se interactúe, se han previsto aplicaciones tecnológicas de seguridad, como los métodos de autenticación[363], mediante los que una entidad externa demuestra su

[360] Artículo 1. Naturaleza y funciones. "1. El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo. 2. Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo. 3. A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general. 4. Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica. 5. La firma electrónica realizada a través del Documento Nacional de Identidad tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel. 6. Ningún español podrá ser privado del Documento Nacional de Identidad, ni siquiera temporalmente, salvo en los casos y forma establecidos por las Leyes en los que haya de ser sustituido por otro documento".

[361] B.O.E. núm. 307, de 24 de diciembre de 2005.

[362] Real Decreto 1586/2009, de 16 de octubre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica. BOE núm. 256, de 3 de noviembre de 2009.

[363] 1.- Autenticación de usuario (PIN): La tarjeta DNIe soporta verificación de usuario (CHV- Card Holder verification). Esta operación es realizada comprobando el código facilitado por la entidad externa a través del correspondiente comando. Cada código CHV tiene su propio contador de intentos. Tras una presentación válida de PIN, el contador de reintentos correspondiente es automáticamente puesto a su valor inicial (típicamente = 3). El contador de intentos es decrementado cada vez que se realiza una presentación errónea, pudiendo llegar a bloquearlo si el contador llega a cero. Es posible desbloquear un código tras una correcta presentación de la huella dactilar del usuario, que en este caso actúa de código de desbloqueo. A su vez estas presentaciones de huellas tienen su propio contador de intentos. Si el número de intentos de presentación de huella dactilar se agota, no será posible realizar la operación de desbloqueo. Es posible cambiar el código de CHV a un nuevo valor presentando el valor actual o presentando la huella dactilar. El código PIN es personal e intransferible, por tanto, únicamente debe ser conocido por el titular de la tarjeta en cuestión.
2.- Autenticación de usuarios mediante datos biométricos: La tarjeta DNIe permite realizar una identificación biométrica del titular de ésta, si bien está función sólo estará disponible en puntos de

identidad, o el conocimiento de algún dato secreto almacenado en la tarjeta, o la securización de mensajes, pues la tarjeta DNIe "permite la posibilidad de establecer un canal seguro entre el terminal y la tarjeta que securice los mensajes transmitidos. Para el establecimiento es necesaria la autenticación previa del terminal y la tarjeta, mediante el uso de certificados. Durante la presencia del canal seguro los mensajes se cifran y autentican, de tal forma que se asegura una comunicación "una a uno" entre los dos puntos originarios del canal. Para el establecimiento del canal seguro, en primer lugar, se realiza un intercambio de las claves públicas de la tarjeta y el terminal mediante certificados que serán verificados por ambas partes. A continuación se realiza un protocolo de autenticación mutua, con intercambio de semillas para la derivación de una semilla común que dé lugar a las claves de sesión de cifrado y autenticado. Una vez concluido el protocolo para el establecimiento de la semilla común todos los mensajes deben transmitirse securizados"[364].

Cuestiones de seguridad más técnicas, son la funcionalidad criptográfica de las claves asignadas a la tarjeta (claves RSA, Hash de datos, y firmas electrónicas), el intercambio de claves (usada para compartir claves simétricas o de sesión entre dos entidades), y el desbloqueo y cambio de PIN, que se ha de realizar siempre en condiciones

---

acceso controlados. La aplicación que accede al DNIe, una vez conocida la información sobre las huellas contenidas en la tarjeta, decide sobre que huella va a proceder a verificar, solicitando al portador que coloque el dedo adecuado. Tras obtener los datos biométricos desde en el dispositivo lector de huellas, presenta la información biométrica a la tarjeta a través del correspondiente comando. Tras las comprobaciones iniciales de condiciones de uso y seguridad, la tarjeta procede, mediante su algoritmo Match on Card, a evaluar la correspondencia entre la huella presentada y la referencia. Si la evaluación supera el umbral, la verificación es correcta. En caso contrario, la tarjeta anota una presentación errónea sobre esa huella devolviendo el número de intentos restantes.
3.- Autenticación de aplicación: El propósito de este método de autenticación es que la entidad externa demuestre tener conocimiento del nombre y valor de un código secreto. Para realizar esta autenticación de aplicación, se utiliza un protocolo de desafío-respuesta, con los siguientes pasos: a) La aplicación pide un desafío a la tarjeta. b) La aplicación debe aplicar un algoritmo a este desafío junto con el correspondiente código secreto y nombre de la clave. c) La tarjeta realiza la misma operación y compara el resultado con los datos transmitidos por la aplicación. d) En caso de coincidir, considera correcta la presentación para posteriores operaciones.
4.- Autenticación mutua: Este procedimiento permite que cada una de las partes (tarjeta y aplicación externa) confíe en la otra, mediante la presentación mutua de certificados, y su verificación. En el proceso, también se incluye el intercambio seguro de unas claves de sesión, que deberán ser utilizadas para securizar (cifrar) todos los mensajes intercambiados posteriormente. Este servicio permite el uso de diferentes alternativas, que podrán seleccionarse implícitamente en función de la secuencia de comandos, o explícitamente, indicando su identificador de algoritmo en un comando de gestión de entorno de seguridad anterior (MSE). Las dos opciones disponibles están basadas en la especificación 'CWA 14890-1 Application Interface for smart cards used as Secured Signature Creation Devices – Part 1', y son la autenticación con intercambio de claves (descrita en el capítulo 8.4 de CWA 14890-1), y la autenticación de dispositivos con protección de la privacidad, (descrita en el capítulo 8.5 de CWA 14890-1).
http://www.dnielectronico.es/Guia_Basica/seguridad.html

[364] Ibidem.

de máxima confidencialidad y en terminales específicamente habilitados a tal efecto o con las debidas condiciones de seguridad (canal seguro). También es posible un cambio de PIN, haciendo uso de la huella dactilar (desbloqueo), únicamente en dispositivos autorizados por la Dirección General de la Policía. Además, por razones obvias, se habrán de tener en cuenta los requisitos de seguridad del entorno[365] en que se trate de operar con el DNI electrónico.

En conclusión, parece que las garantías de seguridad, están previstas tecnológicamente y que el DNI electrónico puede ser utilizado sin temor alguno, sin embargo, siempre queda la pregunta de si los destinatarios de la información contenido en el chip de la tarjeta, habrán implantado las medidas de seguridad necesarias que requiere su tratamiento posterior, y tendrán la formación necesaria sobre su manipulación, para evitar en todo caso un uso no autorizado por terceros, y proteger los derechos de los ciudadanos en materia de protección de datos.

[365] Se han de utilizar los módulos criptográficos CSP y PKCS 11 que se encuentran en la dirección www.dnielectronico.es/descargas/

III. CONTROL ESTATAL DEL CIUDADANO.

1.- Seguridad e intervención de las autoridades.

En el marco de un Estado de Derecho, las Fuerzas y Cuerpos de Seguridad desempeñan sus tareas limitados por los valores y derechos consagrados constitucionalmente, y así, nuestro Tribunal Constitucional señala[366] que:

> "(…) de la Constitución se deduce que las fuerzas de policía están al servicio de la comunidad para garantizar al ciudadano el libre y pacífico ejercicio de los derechos que la Constitución y la Ley les reconocen y este es el sentido del artículo 104.1 CE que puede considerarse directamente heredero del artículo12 de la Declaración de Derechos del Hombre y del Ciudadano, configurando a la Policía como un servicio público para la comunidad, especializado en la prevención y lucha contra la

[366] Sentencia del Tribunal Constitucional nº 55/1990 (F.Jº. 5º).

criminalidad, el mantenimiento del orden y la seguridad pública y la protección del libre ejercicio de los derechos y libertades".

El artículo 104.1 de la Constitución Española señala expresamente la necesidad de que exista un equilibrio entre la definición de Policía como garante de derechos y libertades de los ciudadanos, y su definición como organismo competente para hacer un uso legítimo de la fuerza en la represión de conductas que amenacen la seguridad ciudadana. Dicho equilibrio, habrá de venir fundamentado por el objetivo esencial de preservar el orden constitucional. En la represión de las conductas penalmente sancionables, cuando se utilice la fuerza, se cuidará no menoscabar aquellos derechos o libertades que, en definitiva, se quieren proteger.

La seguridad pública sigue en general unas líneas maestras marcadas por la Constitución y las leyes, y que vienen a delimitar la actuación de las autoridades policiales en materia de prevención y persecución del delito. Sin embargo, la realidad avanza a un ritmo muy diferente del de las normas, y así, dependiendo del ámbito de investigación ante el que nos encontremos, no siempre se podrá hablar de equilibrio con aquellos límites. Habrá situaciones de extrema gravedad, que por su propia naturaleza requieran ser sometidas a una exhaustiva vigilancia por parte de las autoridades pero, utilizar todos los recursos tecnológicos que existen a su alcance, no siempre va a ser proporcionado a los fines perseguidos.

Según BRUCE SCHNEIER, "quien controla nuestros datos, controla nuestras vidas. (…) Nuestros datos son parte de de nosotros. Son íntimos y personales y, tenemos derechos básicos sobre ellos. Deben ser protegidos de tratamientos no consentidos"[367]. Y actualmente, ese control no es ciencia ficción, la tecnología permite supervisar sin necesidad de intervención humana todo tipo de relaciones entre los individuos de una comunidad, simplemente bastaría con controlar todas sus comunicaciones, sin que sus miembros se sepan observados, para obtener flujos de información en

[367] SCHNEIER, BRUCE. *Our Data, Ourselves*, (15 de mayo de 2008). Disponible en: http://www.wired.com/politics/security/commentary/securitymatters/2008/05/securitymatters_0515.

estado puro, que los ciudadanos nunca ofrecerían voluntariamente de saberse interceptados. Sistemas informáticos revelan conexiones entre diferentes puntos geográficos, registros y almacenamiento de datos, identificación del origen y destino de una comunicación, identificación de las personas intervinientes, vigilancia, minería tecnológica de datos, centinelas informáticos, programas espía, etc., y en la actualidad todas estas acciones son muy útiles para configurar un sistema preciso de control de las personas, pero excesivo, es necesario delimitarlo.

Para el control más "eficiente" de la comunidad, incluso pretendiendo el legítimo fin de "la Seguridad del Estado", la información habría de captarse de forma totalmente clandestina, obteniendo palabras y movimientos sin artificios que los deformen o disfracen, más reales que cualquier testimonio provocado, pero lo cierto es que cada vez que una herramienta o un humano "controla" a otro, se vulnera su dignidad, con especial trascendencia, cuando se controla el contenido de sus comunicaciones, o de cualquier otro tipo de información personal[368].

Una muestra del alcance masivo que puede tener este tipo de controles, se puso de manifiesto en Estados Unidos tras los atentados contra las Torres Gemelas. Allí se creó uno de los programas más completos que ha existido nunca para el rastreo de personas, tanto por el volumen de información que pretendía como por los avances técnicos que para ello existían a su disposición, era el programa llamado Total Information Awareness (TIA), desarrollado por el Almirante John M. Poindexter, antiguo asesor de seguridad nacional del Gobierno de Estados Unidos (1983-1986). Poindexter se encargó, como responsable de Proyectos de Investigación Avanzada de Defensa (DARPA), de introducir en la Casa Blanca las nuevas tecnologías como parte imprescindible de los programas de seguridad estatal. Trató de implantar un sistema único de control de información integrado por distintos departamentos y programas con el objetivo único de

[368] MARKOFF,J. Ex - responsable de investigaciones de delitos informáticos del Departamento de Justicia del Gobierno de los Estados Unidos y vicepresidente primero de Solutionary, Inc., una compañía de seguridad electrónica ubicada en Omaha, Nebraska (EEUU). Noticia aparecida en el diario *El País*, 09-03-2006. Disponible en: http://www.elpais.com/solotexto/articulo.html?xref=20060309elpepunet_5&type=Tes&k=vigilancia_electronica_pone_peligro_libertades_civiles#noticias

"controlar" información aprovechando al máximo los avances informáticos de todo tipo de áreas, y siempre al servicio de la seguridad[369]. En el resto del mundo también se han invertido miles de millones en procurar conocer todas las posibilidades de las tecnologías "espía", y cada vez más enfocada a la vigilancia de Internet y de las comunicaciones electrónicas. Para cualquier gobierno, delimitar el alcance del progreso tecnológico en lo material es imposible, sin embargo, en lo que respecta a su "espíritu", a su utilización, si debe ser previsto y ejecutado, en cuanto que su finalidad última y las personas al servicio de quienes realmente se implanta, es lo que debe guiar todo proyecto de defensa estatal: buscar la proporcionalidad y el respeto a un desarrollo digno del ser humano.

La realidad nos muestra que en la implantación de medidas de seguridad contra los diversos tipos de amenazas, los Estados cada vez están prescindiendo más de considerar el resultado global de sus actuaciones en favor de la protección de la comunidad, a veces incluso, aparente. Los Estados, cada vez más preocupados por los ataques terroristas, que puedan sesgar el régimen de bienestar social en que se desenvuelve la comunidad que los habita, toman medidas extremas de control para supervisar agentes o movimientos potencialmente peligrosos. No se duda en restar cada vez mayores parcelas de la integridad del ser humano, observando minuciosamente todos y cada uno de sus movimientos, pero vigilan a todos, sospechosos e innecesarios, limitando la libertad natural de movimientos de la comunidad de forma genérica e indiscriminada.

La realización de minerías libres de informaciones obtenidas a través de la tecnología bajo un pretendido "control" de riesgos, puede acabar convirtiendo al Estado en un almacén masivo de ficheros de datos

[369] Conocimiento Total de la Información. Este programa fue creado en Estados Unidos en Febrero de 2003, y fue renombrado como Terrorism Information Awareness en Mayo, pasando después a formar parte del Programa de la Agencia de proyectos de investigación avanzada de Defensa (DARPA). Disponible en: http://infowar.net/tia/www.darpa.mil/iao/index.htm y en, http://www.darpa.mil/. Estaba configurado por distintas unidades, que pretendían (y pretenden) controlar la mayor cantidad de información y comunicaciones posible, a favor de la seguridad del Estado. Estas unidades son Genysis, para la interconexión de bases de datos; Genoa y Genoa II, para la investigación del contenido de esas bases de datos; Comunicator, para controlar comunicaciones en el campo de batalla; TIDES y Babylon para las traducciones; FutureMap, para predicción de futuros comportamientos aplicados en base a estudios de mercado; EELD, para la interpretación de las informaciones recabadas; EARS, para transformar en texto las comunicaciones verbales; Biovigilancia, para identificación de factores biológicos; Identificación humana a distancia (HID) y, Simulación de ambientes asimétricos (WAE).

personales que en realidad nunca se llegan a utilizar para los fines que los crearon y si, pueden llegar a ser manipulados para otros usos no tan lícitos. Aunque efectivamente ese "almacén" fuese creado con un objetivo de carácter primario, de supervivencia de la comunidad, la realidad está poniendo de manifiesto que acometer esta tarea sin poner límites de carácter humano, conlleva registros masivos, indiscriminados, y generalmente innecesarios, de todo tipo de información, de tal forma que se puede provocar un efecto altamente invasivo en la esfera personal de los ciudadanos, desbordando su función original: preservar la seguridad de la comunidad.

Por todo ello, en toda intervención policial se debe exigir la protección de los ciudadanos, un escrupuloso respeto de sus derechos y libertades[370]. Pero el problema está en la eficacia real, en conseguir los máximos beneficios con el menor riesgo o coste posible para aquellos a quienes en realidad se debe proteger.

En la Memoria que precedía a la presentación del Proyecto de Ley de Seguridad de 1979[371], en su apartado II, se señalaba expresamente que las intervenciones preventivas de situaciones que alterasen de forma grave el orden y la seguridad, por parte de la Autoridad Gubernativa y sus Agentes, debían abordarse siempre dentro del marco de la Constitución: "De esta forma se concilia la protección de los derechos y libertades y la garantía de la seguridad ciudadana, pues es obvio que esta no puede quedar indiferente frente al ejercicio abusivo e ilegal de aquellos, ni el recto ejercicio de los derechos y libertades puede impedirse ni restringirse arbitrariamente".

En el apartado VII continuaba esta Memoria diciendo que "la lucha contra el terrorismo se sustenta sobre dos pilares básicos: de una parte, la acción de investigación, identificación y detención de los responsables, por

[370] "Necesitamos una ley de protección de datos efectiva, que proteja toda la información sobre las personas y no se limite sólo a la información financiera o de salud. Debería limitar la capacidad de otros de comprar y vender nuestra información sin nuestro conocimiento y consentimiento. Debería permitirnos ver la información que sobre nosotros tienen otros, y corregir cualquier inexactitud que encontremos. Debería impedir al gobierno rastrear nuestra información sin control judicial. Debería obligar a la cancelación de datos y limitar su recopilación. Necesitamos algo más que penas simbólicas por vulneraciones deliberadas" .SCHNEIER, B*. Our Data, Ourselves... Op. Cit.*

[371] Boletín Oficial de las Cortes Generales Nº73-I, de 29 de Septiembre de 1979.

cualquier concepto, de tan grave modalidad de delincuencia, que queda confiada a la Autoridad gubernativa y, de otra, la acción punitiva, de procesamiento y condena, que se encomienda a la Autoridad judicial (…) Para el logro de tales objetivos se han ido dictando en los últimos meses todo un conjunto de medidas legislativas que han afectado indistintamente, de una parte a la legislación penal propiamente dicha (Código Penal y Ley de Enjuiciamiento Criminal) y, de otra, a la legislación sobre orden público y seguridad ciudadana (…). Sobre esta situación legislativa ha venido a incidir la Constitución, obligando, desde la superioridad de su rango normativo a un replanteamiento y adecuación a sus mandatos de toda la normativa preexistente, por cuya razón se ha procedido a incorporar, dentro del presente proyecto de ley, el desarrollo legislativo adecuado de su artículo 55.2"[372].

Sin embargo, el respeto a la Constitución, de obligado cumplimiento para el poder legislativo, se está desfigurando en los últimos años de forma muy negativa por el incremento de la delincuencia organizada y del terrorismo, por la amenaza que suponen para el bienestar social. El objetivo "evitar riesgos" ha complicado la delimitación correcta de los instrumentos y facultades de que deberían disponer las autoridades policiales para combatirlos, para su investigación o para su prevención. En vez de atenderse a la proporcionalidad de las medidas y los fines perseguidos, últimamente parece que todo vale en favor de un absoluto control gubernativo de cada movimiento humano.

Si bien la Constitución es consciente de la necesidad de ajustar la ejecución de sus garantías, con una debida ponderación de los intereses a proteger, el legislador no siempre lo está teniendo en cuenta al desarrollarla. Por ejemplo, en la referida Memoria se explicaba que "es de destacar, en primer lugar, cómo la norma suprema del Estado se hace

[372] Artículo 55.2 de la CE: "Una Ley Orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. La utilización injustificada o abusiva de las facultades reconocidas en dicha Ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las Leyes".

beligerante en la acción contra el terrorismo, autorizando, al margen de la declaración de los estados de excepción y sitio, la suspensión de los derechos fundamentales que menciona, a determinadas personas, siempre que tal suspensión guarde relación de medio a fin "con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas" y que los eventuales riesgos que tal medida suponga para las libertades ciudadanas queden debidamente contrarrestadas con las correlativas garantías que asimismo arbitra: "Necesaria intervención judicial y adecuado control parlamentario", siquiera tales controles y garantías, por la propia naturaleza de la suspensión sobre la que recaen, y para no dañar su eficacia, deban ser "a posteriori" y no preventivos". En la actualidad, muchas de las normas que restringen el ejercicio de derechos fundamentales en determinadas situaciones, no prevén correlativamente mecanismos ágiles de reparación de los daños que pudieran producirse por aquellas intervenciones extraordinarias, quedando en manos de los ciudadanos valorar posibles efectos irreversibles de su indiferencia.

1.1.- Ley de Seguridad Ciudadana.

En un Estado Democrático de Derecho, la "seguridad ciudadana" es el resultado material de la vigencia efectiva de determinados derechos fundamentales, entre ellos singularmente la libertad personal (17.1 CE); pero también es el resultado de la existencia real de un régimen de seguridad jurídica (artículo 9.3 CE). Es indiscutible que la Constitución asigna un papel sin duda relevante a las Fuerzas y Cuerpos de Seguridad del Estado, pero siempre con carácter instrumental, dentro de aquéllas coordenadas[373].

[373] Ahora bien, cuando como aquí acontece ese papel resulta sobredimensionado y la «seguridad ciudadana» se convierte abusivamente en un fin en sí, la policía deja de ser función de garantía de los derechos y libertades, para transformarse ella misma en un nuevo y cualificado factor de inseguridad. Declaraciones del IV Congreso de "Jueces para la Democracia", *Sobre el proyecto de Ley Orgánica sobre protección de la Seguridad Ciudadana.* Logroño, 1991. Disponible en: http://www.juecesdemocracia.es/congresos/vicongreso/declaraciones/Sobre%20el%20proyecto%20de%20Ley%20Org%A0nica%20sobre%20Portecci%A2n%20de%20la%20S%85.pdf

En este sentido, los trabajos parlamentarios para el desarrollo de las previsiones de la Constitución Española, que venían a sustituir las directrices habidas hasta el momento en el régimen dictatorial español, en materia de seguridad de Estado y ciudadanía, se plasmaron a partir de 1979 en un Proyecto de Ley de Seguridad Ciudadana, que fue publicado en el Boletín Oficial de las Cortes Generales, el día 21 de septiembre de 1979. Contenía 72 artículos, dos disposiciones adicionales, dos disposiciones derogatorias y cuatro disposiciones finales que regulaban materias relativas a las competencias de las autoridades gubernativas (Cap. I), a la prevención y mantenimiento de la seguridad ciudadana (Cap. II), al estado de alarma, de excepción y sitio (Cap. III), a las potestades gubernativas especiales en relación con los supuestos previstos en el artículo 55.2 de la Constitución[374] (Cap. IV) y a las Fuerzas y cuerpos de seguridad del Estado (Cap. V).

En los inicios de la elaboración del Proyecto, tras el trámite de enmiendas, se aceptó una enmienda especial, de carácter estructural, que fue presentada por el Grupo Parlamentario Comunista, y que proponía a la Comisión que el proyecto de Ley se dividiese en otros cuatro proyectos que podrían tramitarse de forma independiente. Y así fue, los trabajos se estructuraron en cuatro partes:

1. Ley de Seguridad Ciudadana y competencias gubernativas.
2. Ley orgánica de los estados de alarma, excepción y sitio.
3. Ley orgánica sobre los supuestos previstos en el artículo 55.2 de la Constitución.
4. Ley orgánica de las Fuerzas y Cuerpos de Seguridad.

La propuesta fue aprobada por la Comisión Constitucional y, publicada en el Boletín Oficial de las Cortes Generales el 27 de enero de 1980.

[374] Artículo 55.2 CE: "Una Ley Orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. La utilización injustificada o abusiva de las facultades reconocidas en dicha Ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las Leyes".

En materia de seguridad de Estado y ciudadanía, la "Ley de Seguridad Ciudadana"[375], más conocida como la "Ley Corcuera", fue aprobada en el año 1992 bajo la premisa del respeto a la CE y, con el reconocimiento expreso de que "la protección de la seguridad ciudadana y el ejercicio de las libertades públicas constituyen un binomio inseparable, y ambos conceptos son requisitos básicos de la convivencia en una sociedad democrática"[376]. Esta norma vino a sustituir, no sin polémica[377], a la emblemática Ley de Orden Público del régimen franquista, pues en ese momento ya resultaba completamente ajena a la instaurada Democracia. Procedía desarrollar la CE y regular las competencias para la protección del libre ejercicio de los derechos y libertades y de las garantías de la seguridad ciudadana, y las competencias de las Fuerzas y Cuerpos de Seguridad, que fueron otorgadas de conformidad con el artículo 104.1 CE.

En concreto, el proyecto dedicado a la Seguridad Ciudadana constaba de cuatro partes claramente diferenciadas: la relativa a las autoridades gubernativas, sus competencias y funciones en situaciones normales; la relativa a las facultades extraordinarias y límites en los estados de alarma, excepción y sitio; la relativa a las facultades gubernativas para la suspensión de derechos en la lucha contra bandas armadas y terroristas y, la cuarta, la relativa a las funciones, principios de actuación y estatutos de los Cuerpos de Seguridad del Estado.

Entre las directrices de actuación que recogía dicha norma, las que detallaban los procedimientos para la identificación de las personas[378] provocaron una firme oposición[379] en la doctrina, porque reconocían que determinadas unidades de carácter administrativo podían, en el ejercicio de sus funciones, llegar a afectar al ejercicio de algunos derechos fundamentales, como "el derecho a la libertad, a la libre circulación por el territorio nacional y a entrar y salir libremente de España o al derecho de

[375] Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana.
[376] Ibdem. Exposición de Motivos.
[377] FERNÁNDEZ ENTRALGO, J. *Seguridad Ciudadana. Materiales de Reflexión. Crítica sobre la Ley Corcuera*. Ed. Trotta. Madrid, 1993, y, la no menos polémica, Sentencia nº 341/1993, de 18 de Noviembre, del Tribunal Constitucional, en resolución de los Recursos de Inconstitucionalidad nº 1. 045/1992,1. 279/1992 y 1. 314/1992 y, Cuestiones de Inconstitucionalidad 2. 810/1992 y 1. 372/1993.
[378] Artículo 20 y ss. de la LOPSC.
[379] FAIRÉN GUILLÉN, V. *La identificación de personas desconocidas.* Ed. Civitas. Madrid, 1992. p. 51 y ss.

reunión"[380]. Podían hacerlo aparentemente sin demasiadas garantías y a pesar de que se estableció "el ámbito de responsabilidad de las autoridades administrativas en materias como la fabricación, comercio, tenencia y uso de armas y explosivos; concentraciones públicas en espectáculos; documentación personal de nacionales y extranjeros en España; así como regular ciertas actividades de especial interés y responsabilidad para las Fuerzas y Cuerpos de Seguridad". La Ley además regulaba estas posibilidades respecto las actividades relacionadas con armas y explosivos, "habilitando la intervención del Estado en todo el proceso de producción y venta, así como en la tenencia y uso de los mismos"; las actividades en materia de espectáculos públicos y actividades recreativas, "dejando a salvo las competencias que, en este punto, tienen reconocidas las Comunidades Autónomas mediante sus correspondientes Estatutos; los supuestos de desórdenes colectivos o de inseguridad publica graves, quedando facultadas las autoridades para el cierre de locales o establecimientos y para la evacuación de inmuebles en situaciones de emergencia o en circunstancias que lo hagan imprescindible" y, para limitar o restringir la circulación o permanencia en vías o lugares públicos, en supuestos de alteración del orden o la seguridad ciudadana. Se posibilitaba asimismo el establecimiento de controles en las vías, lugares o establecimientos públicos, con el fin de descubrir y detener a los partícipes en un hecho delictivo y de aprehender aquellos instrumentos, efectos o pruebas que pudieran encontrarse del mismo.

En materia de control y/o registro de datos personales de los ciudadanos afectados, esta Ley destaca por haberles dotado de un nuevo

[380] STC 341/1993, de 18 de Noviembre. (F.Jº 8º y 9º): 8.- (…) "El que la Ley no haya articulado para las diligencias de identificación un límite temporal expreso no supone una carencia que vicie de inconstitucionalidad al precepto; lo sustantivo es que el legislador limite temporalmente esta actuación policial a fin de dar seguridad a los afectados y de permitir un control jurisdiccional sobre aquella actuación, finalidades, una y otra, que quedan suficientemente preservadas en el enunciado legal sometido a nuestro control: la fuerza pública sólo podrá requerir este acompañamiento a «dependencias próximas y que cuenten con medidas adecuadas para realizar las diligencias de identificación» y las diligencias mismas, en todo caso, no podrán prolongarse más allá del «tiempo imprescindible» para la identificación de la persona. Precisión que implica un mandato del legislador de que la diligencia de identificación se realice de manera inmediata y sin dilación alguna [F.J. 6]. 9.- No resulta inexcusable que la identificación misma haya de llevarse a cabo necesariamente en presencia o con la asistencia de Abogado, garantía ésta cuya razón de ser está en la protección del detenido y en el aseguramiento de la corrección de los interrogatorios a que pueda ser sometido (STC 196/1987). Ninguna de estas garantías constitucionales -recordatorio del derecho a no declarar y asistencia obligatoria de Abogado- son indispensables para la verificación de unas diligencias de identificación que, vale reiterar, no permiten interrogatorio alguno que vaya más allá de la obtención de los "datos personales" a los que se refiere el repetido artículo 9.3 de la L.O.P.S.C. [F.J. 6]". (…)

"derecho – deber": el de estar identificado en todo momento, el "de obtener el Documento Nacional de Identidad a partir de los catorce años, que tendrá por sí solo suficiente valor para acreditar la identidad de los ciudadanos, garantizando en todo caso el respeto al derecho a la intimidad de la persona, sin que los datos que en el mismo figuren puedan ser relativos a raza, religión, opinión, ideología, afiliación política o sindical, o creencias. Y regulaba además, las condiciones en que los agentes de las Fuerzas y Cuerpos de Seguridad, siempre que ello fuese necesario para el ejercicio de las funciones de protección de la seguridad que les corresponden, podrán requerir la identificación de las personas"[381]. Con esta previsión, supuestamente no se alteraba el régimen que previsto en aquel momento para las detenciones, "que solo podrá seguir produciéndose cuando se trate de un sospechoso de haber cometido un delito y no por la imposibilidad de identificación", sin embargo la norma matizaba en su articulado estos supuestos hasta tal punto que[382], se previeron "supuestos de resistencia o negativa infundada a la identificación, que tendrían las consecuencias que para tales infracciones derivan del Código Penal vigente". También se regulan "las condiciones y términos en que, conforme a lo permitido por la Constitución y las Leyes, podrá prescindirse del mandamiento judicial para penetrar en domicilios, en lo que se refiere a las tareas de persecución de fenómenos delictivos"[383].

La Ley de Seguridad Ciudadana es una norma que vino a completar el régimen policial esbozado en la Constitución. Según la propia norma, "las Cortes Generales han tratado de mantener un positivo equilibrio entre libertad y seguridad, habilitando a las autoridades correspondientes para el cumplimiento de sus deberes constitucionales en materia de seguridad, mediante la aprobación de Leyes Orgánicas Generales como la de 1 de junio

[381] Continúa la Exposición de Motivos: (...) "Si no pudieran identificarse por cualquier medio, podrán ser instadas a acudir a una dependencia policial próxima a los solos efectos de la identificación".

[382] FAIRÉN GUILLÉN, V. *La identificación de personas desconocidas.* …, Op. Cit. p. 57. (…) "Y el desobedecer a un requerimiento del agente de la autoridad a "acompañar", pese a los equilibrios dialécticos efectuados en el Parlamento, "el negarse a acompañarlo", en principio, es una desobediencia a una autoridad. Pero el artículo20.4 habla de la "negativa infundada" a la identificación. Esto es, el ciudadano requerido, podrá negarse de manera fundamentada, razonada, dirigiéndose al requirente y así, no "acompañarlo" a la comisaría sin incurrir en desobediencia. Si esto es así (ya que dudo de esta misma conclusión provisional: lo que indica lo irritantes que son los textos equívocos o proclives a la cavilosidad, sobre todo cuando se trata de libertad de movimientos) (…) ¿Qué debe ocurrir? Nada de eso figura en el texto legal".

[383] Se refiere en este punto, la Exposición de Motivos, al ejemplo de la investigación del narcotráfico.

de 1981, de los Estados de alarma, excepción y sitio; la de 1 de julio de 1985, sobre Derechos y libertades de los extranjeros en España, o la de 13 de marzo de 1986, de Fuerzas y Cuerpos de Seguridad. Asimismo, se han aprobado Leyes Especiales, como la de 15 de julio de 1983, Reguladora del Derecho de Reunión; la de 21 de enero de 1985, sobre Protección Civil, o la de 25 de julio de 1989, de Bases sobre Tráfico, circulación de vehículos a motor y seguridad vial; incluyéndose, asimismo, medidas de prevención de la violencia en los espectáculos deportivos mediante la Ley 10/1990, de 15 de octubre, del Deporte, que dedica a la materia su Título IX".

Se pretendía por primera vez en territorio español, facilitar y orientar "la tarea de proteger un ámbito de seguridad y convivencia en el que sea posible el ejercicio de derechos y libertades, mediante la eliminación de la violencia en las relaciones sociales y la remoción de los obstáculos que se opongan a la plenitud de dichas libertades y derechos", aunque lo cierto es que supuso el comienzo de un proceso cada vez más restrictivo de control y supervisión estatal, que finalmente hoy parece haberse aceptado socialmente como algo necesario, sin apenas oposición, desde los graves sucesos terroristas que han ocurrido a nivel internacional, y que por primera vez con fecha 11 de Septiembre de 2001, conmocionaron a la población mundial como nunca antes[384]. Desde entonces otras muchas normas han sido promulgadas con esa misma intención de proteger a los ciudadanos, por ejemplo, las relativas a la videovigilancia[385], a la protección de datos de carácter personal[386], a la creación de bancos genéticos[387], a la seguridad de los espectáculos deportivos[388], a la seguridad aérea[389], etc. Para prevenir situaciones que antes se consideraban de extrema excepcionalidad, se están trabajando procedimientos de exhaustivo control social, beneficiado sin duda por el progresivo desarrollo de la tecnología.

---

[384] En especial, han sido decisivos para una conciencia global en materia de Seguridad de Estado, los atentados terroristas del 11 de Septiembre de 2001 en Nueva York, los del 11 de Marzo de 2004 en Madrid y, los del 7 de Julio de 2005 de Londres.

[385] Ley orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares público.

[386] La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

[387] Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

[388] Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.

[389] Ley 21/2003 de 7 de julio, de Seguridad Aérea.

1.2.- Estado de Sitio, de Alarma y, de Excepción.

Como ya se ha señalado, otro de los apartados de la Ley de Seguridad Ciudadana que se estaba elaborando en 1979 era la Ley Orgánica de los estados de alarma, excepción y sitio. Este proyecto recogía las competencias y procedimientos para la declaración de cada uno de dichos estados y, determinaba qué derechos de los ciudadanos podían ser suspendidos o, los deberes de los ciudadanos en los casos de grave riesgo.[390]

También estableció medidas de carácter preventivo, que debían adoptarse contra las perturbaciones de la seguridad ciudadana, y que en todo caso se pretendía fueran tomadas sin merma de las libertades establecidas en la Constitución.

Preservar el equilibro del Estado de Derecho ha sido una prioridad desde que en España se instaurara la democracia, tras las primeras elecciones, celebradas el 15 de junio de 1977. De hecho, la Constitución de 1978, recogió expresamente la posibilidad de que se dieran situaciones extremas, y que por ello su propia vigencia se pudiera ver limitada en aras, única y exclusivamente, de la restitución del orden alterado. En este sentido, "el modelo de Derecho de excepción que se recoge en nuestra Constitución se construye sobre la previsión de que puedan surgir determinadas situaciones de crisis que requieren que determinados contenidos constitucionales sean suspendidos durante un tiempo limitado a la espera de que se solucione la emergencia que podrá responder al estado de alarma, de excepción o de sitio. En ningún caso, se prevé una

[390] "Asimismo, como expresión de las garantías que deben preceder y acompañar la aplicación del ordenamiento excepcional, el artículo 55 de la propia Constitución determina expresamente, por vía enumerativa y con carácter excluyente, cuáles son los derechos fundamentales y cuáles las libertades públicas que podrán ser suspendidas cuando se produzca alguna de las circunstancias que lleva a la declaración de los estados de excepción y sitio (Rumores)". Diario de Sesiones del Congreso de los Diputados, nº 160. Sesión Plenaria del Congreso de los Diputados, de 21 de abril de 1981. Debate sobre el Dictamen de la comisión constitucional sobre el proyecto de ley orgánica reguladora de los estados de alarma, excepción y sitio. Intervención del Ministro del Interior, Rosón Pérez. p. 9875

suspensión total de la Constitución, ni mucho menos, pues solamente se podrán suspender los derechos enumerados en el artículo 55 cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución"[391].

TORRES MURO lo expresa diciendo que "hay una "Constitución suspendible" (derechos previstos en el artículo 55 CE), y el resto es resistente a la excepción, como consecuencia de que el principio estructural básico en el modelo de estado excepcional adoptado es el de enumeración, de modo que el fenómeno de la suspensión de garantías solamente puede extenderse a los derechos de los que hemos hablado, de cuya importancia nadie duda (libertad personal, libertad de expresión e información, reunión, huelga...) pero que no son todos los constitucionales. Diversificado, porque el artículo 116 prevé tres tipos de estados excepcionales, dedicados cada uno de ellos a responder a situaciones diferentes (...)"[392].

Este artículo 116, señala literalmente:

"1. Una Ley orgánica regulará los estados de alarma, de excepción y de sitio y las competencias y limitaciones correspondientes.

2. El estado de alarma será declarado por el Gobierno mediante decreto acordado en Consejo de Ministros por un plazo máximo de quince días, dando cuenta al Congreso de los Diputados, reunido inmediatamente al efecto y sin cuya autorización no podrá ser prorrogado dicho plazo. El decreto determinará el ámbito territorial a que se extienden los efectos de la declaración.

3. El estado de excepción será declarado por el Gobierno mediante decreto acordado en Consejo de Ministros, previa

[391] ABA CATOIRA, A. "El Estado de Alarma... Op. Cit. p. 323.
[392] TORRES MURO, I. *Artículo 116 CE: Los estados excepcionales.* En CASAS BAAMONDE, Mª E., y RODRÍGUEZ – PIÑERO Y BRAVO – FERRER, M. (Directores). Comentarios a la Constitución Española... Op. Cit. pp. 1814 – 1820.

autorización del Congreso de los Diputados. La autorización y proclamación del estado de excepción deberá determinar expresamente los efectos del mismo, el ámbito territorial a que se extiende y su duración, que no podrá exceder de treinta días, prorrogables por otro plazo igual, con los mismos requisitos.

4. El estado de sitio será declarado por la mayoría absoluta del Congreso de los Diputados, a propuesta exclusiva del Gobierno. El Congreso determinará su ámbito territorial, duración y condiciones.

5. No podrá procederse a la disolución del Congreso mientras estén declarados algunos de los estados comprendidos en el presente artículo, quedando automáticamente convocadas las Cámaras si no estuvieren en período de sesiones. Su funcionamiento, así como el de los demás poderes constitucionales del Estado, no podrán interrumpirse durante la vigencia de estos estados.

Disuelto el Congreso o expirado su mandato, si se produjere alguna de las situaciones que dan lugar a cualquiera de dichos estados, las competencias del Congreso serán asumidas por su Diputación Permanente.

6. La declaración de los estados de alarma, de excepción y de sitio no modificará el principio de responsabilidad del Gobierno y de sus agentes reconocidos en la Constitución y en las Leyes”.

Se trata de prever la defensa política de la Constitución, frente a situaciones excepcionales, para las que el Derecho ordinario no tiene respuesta suficiente. CRUZ VILLALÓN, dice que la Constitución cobija una concepción de la realidad social que se considera normal y, si esta cambia,

aquella ha de ser capaz por si misma de garantizar su propia eficacia[393], ofreciendo "los medios jurídicos necesarios para su protección y permanencia". Para el "mantenimiento del normal funcionamiento de las instituciones", ante una alteración de la convivencia democrática, se deberán adoptar las "medidas estrictamente indispensables para solucionar la crisis declarada". Con esta garantía la Constitución introduce los principios de "presunción de legitimidad de la actuación del Estado" y el de "responsabilidad del poder que está sometido a limitaciones en su ejercicio y a un posterior control"[394], porque son situaciones excepcionales en las que se va a concentrar el poder en manos del Poder Ejecutivo, suspendiéndose la aplicación de algunas previsiones constitucionales propias del Estado de derecho.

El Derecho de excepción es necesario, porque una "garantía diacrónica del orden público configurado por la Constitución para supuestos de crisis constitucional que superan la capacidad normativa de la Constitución. Esta incapacidad, sin embargo, y es aquí donde comienza el problema, no resulta exclusivamente de lo excepcional de una situación todavía no precisada en cuanto a su contenido, sino de la combinación de esta última con el contenido específico de la Constitución. Porque la Constitución (...) es un proyecto de organización de un poder político que se quiere a si mismo limitado (...)[395]". Ahora bien, también hay que tener en cuenta que "el riesgo de incorporar la suspensión de la Constitución como una garantía de la misma es en todo caso mayor que el derivado de la ausencia de un derecho de excepción[396]" y crear por ello, un sistema equilibrado, que recoja aquellas situaciones que se consideran excepcionales para poder declarar el estado excepcional, que establezca el

[393] CRUZ VILLALÓN, P. *Estados excepcionales y suspensión de garantías*. Ed. Tecnos. Madrid, 1984. p.17.
[394] "Quiero con esto decir que es absolutamente necesaria la existencia de estas normas para evitar que el Estado democrático, intentando defenderse frente a amenazas o ataques que persiguen su desestabilización o fractura, se autodestruya haciendo tambalear los pilares sobre los que se asienta el Estado de Derecho, esto es, el imperio de la Ley, la separación de poderes y el reconocimiento y garantía de los derechos y libertades de la ciudadanía". ABA CATOIRA, A. "El Estado de Alarma en España". *Teoría y Realidad Constitucional* nº 28. UNED. 2011. p. 316. Disponible en: http://e-spacio.uned.es/fez/eserv.php?pid=bibliuned:TeoriayRealidadConstitucional-2011-28-2080&dsID=Documento.pdf
[395] CRUZ VILLALÓN, P. *Estados excepcionales y suspensión*... Op.Cit. p. 13. En contraposición a estas garantías están aquellas otras que denomina "diatópicas" en el sentido de que la Constitución contiene un sistema inmanente de garantía, como por ejemplo la estructuración del poder político, que tiene una eficacia permanente.
[396] Ibídem. p. 28.

procedimiento formal de declaración de la crisis y, las medidas a adoptar para reestablecer la situación de normalidad.

Y, en desarrollo del precepto constitucional, para preservar el interés general y la pronta recuperación de la normalidad, se promulgó la Ley Orgánica 4/1981, de 1 de junio, de los Estados de Alarma, Excepción y Sitio.

Esta norma recoge en sus tres primeros artículos previsiones de aplicación general a los supuestos de estados excepcionales, y aunque cada uno tiene su propia naturaleza y particularidades, deben respetar una serie de principios básicos encaminados a mantener en lo posible el funcionamiento de los poderes públicos y a garantizar en todo caso, el ejercicio de los derechos y libertades individuales constitucionalmente establecidos. Por ejemplo, según el apartado primero del artículo 1 de la Ley Orgánica 4/1981, de 1 de junio, procederá la declaración de los Estados de Alarma, Excepción o Sitio "cuando circunstancias extraordinarias hiciesen imposible el mantenimiento de la normalidad mediante los poderes ordinarios de las autoridades competentes". Es decir, han de darse circunstancias verdaderamente excepcionales, porque las medidas que se podrán adoptar, van a ser igualmente excepcionales. Por eso precisamente dice: "las medidas a adoptar en los Estados de Alarma, Excepción y Sitio, así como la duración de los mismos, serán en cualquier caso las estrictamente indispensables para asegurar el restablecimiento de la normalidad. Su aplicación se realizará en forma proporcionada a las circunstancias" (apartado segundo). Es decir, las medidas que se adopten han de ser "necesarias" y, su aplicación se hará de forma "proporcionada" a las circunstancias y a los fines de seguridad que, en todo caso, se pretendan[397]. Otros principios informadores de este régimen especial son la limitación temporal y la publicidad. El primero, se prevé en el sentido de

[397] "Estos principios de necesidad y utilidad exigen una aplicación proporcionada de las medidas previstas a las circunstancias excepcionales. Ello obedece a que el principio de proporcionalidad vigente en un Estado democrático que exige el respeto a la dignidad humana, distingue dos aspectos: Por una parte, la necesidad misma de que la pena sea proporcionada al delito. Por otra parte, la exigencia de que la medida de la proporcionalidad se establezca en base a la importancia social del hecho (a su nocividad social)". Bru Peral, E.V., citando a MIR PUIG, S., en "Estados de alarma, excepción y sitio". Derechos y Libertades. *Revista del Instituto de Derechos Humanos Bartolomé de las Casas. Universidad Carlos III.* Nº 7 – Madrid, 1999. p. 143.
Disponible en: http://e-archivo.uc3m.es/dspace/bitstream/10016/1354/1/DyL-1999-IV-7-Bru.pdf

que las medidas a adoptar durante la vigencia de uno de estos estados deben tener carácter temporal, tener la duración estrictamente indispensable y proporcional a las circunstancias existentes, hasta que sea efectiva la restauración de la normalidad. El segundo, implica que las medidas adoptadas deben publicarse en el Boletín Oficial del Estado, momento en que entrarán en vigor, y ser difundidas por los medios de comunicación tanto públicos como privados. Aunque también "serán de difusión obligatoria las disposiciones que la autoridad competente dicte durante la vigencia de cada uno de dichos estados"[398]. A pesar de lo extraordinario de estas medidas, se prohíben los tribunales de excepción, o sea, "los actos y disposiciones de la Administración Pública adoptados durante la vigencia de los Estados de Alarma, Excepción y Sitio serán impugnables en vía jurisdiccional de conformidad con lo dispuesto en las Leyes", manteniéndose en todo caso la tutela judicial efectiva[399].

En cuanto a las medidas a adoptar, habrá de estarse a las concretas circunstancias de cada momento, en atención a preservar el orden público bajo el marco que establece para ello la Constitución[400].

Bajo el Estado de Alarma[401], previsto cuando se hayan dado alteraciones graves de la normalidad, como catástrofes, calamidades o desgracias públicas, tales como terremotos, inundaciones, incendios urbanos y forestales o accidentes de gran magnitud; crisis sanitarias, como epidemias y situaciones de contaminación graves; paralización de servicios públicos esenciales para la comunidad o situaciones de desabastecimiento de productos de primera necesidad, se podrán adoptar medidas

[398] Artículo 2 de la Ley Orgánica 4/1981, de 1 de junio.

[399] Artículo 117. 6 de la CE: *Se prohíben los Tribunales de excepción.*

[400] (...) "si es cierto, también, que el derecho de excepción español, tal y como lo configura el artículo que hemos comentado, es un ejemplo de cómo se puede atender a la preservación de la "salus pública" con métodos plenamente constitucionales". TORRES MURO, I. *Conclusiones. Los estados excepcionales*. En CASAS BAAMONDE, Mª E., y RODRÍGUEZ – PIÑERO Y BRAVO – FERRER, M. (Directores). Comentarios a la Constitución Española… Op.Cit. p. 1819.

[401] BRU PERAL, E.V., "Estados de alarma, excepción y sitio"… Op. Cit. p. 153. La declaración del Estado de Alarma habrá de estar motivada por estas circunstancias y, "deberá contener una regulación detallada del tiempo, forma, lugar, competencias, efectos que tendrá, ya que el derecho de excepción es una protección reforzada del ordenamiento constitucional, y un mecanismo del estado de derecho para regular las situaciones de anormalidad y conseguir la vuelta a la normalidad".

encaminadas a garantizar servicios mínimos de rescate, de atención sanitaria, o de actividad en servicios públicos como el transporte[402].

Bajo el Estado de Excepción, que se decretará "cuando el libre ejercicio de los derechos y libertades de los ciudadanos, el normal funcionamiento de las instituciones democráticas, el de los Servicios Públicos esenciales para la comunidad, o cualquier otro aspecto del orden público, resulten tan gravemente alterados que el ejercicio de las potestades ordinarias fuera insuficiente para restablecerlo y mantenerlo*"* (Artículo 13 de la Ley Orgánica 4/1981, de 1 de junio)[403], se prevé

[402] La naturaleza jurídica del Estado de Alarma reconoce una doble finalidad: responder con eficacia frente a las grandes catástrofes naturales y, responder con rapidez frente a una emergencia de orden público. Abarca por tanto situaciones con origen en conflictos sociales o bien de origen natural, pero que supongan un peligro la subsistencia física de la comunidad, situaciones que supongan una alteración grave del orden público y que no hagan necesaria la declaración del Estado de Excepción. Artículo 4 de la Ley Orgánica 4/1981, de 1 de junio. Se refiere a estas situaciones especiales y, en concreto, a "la paralización de los servicios públicos esenciales para la comunidad, cuando no se garantice lo dispuesto en los artículos 28.2 y 37.2 de la Constitución", es decir, cuando no se garantice en el ejercicio del derecho a la huelga de los trabajadores para la defensa de sus intereses o, cuando no se garantice en el ejercicio del derecho de los trabajadores y empresarios a adoptar medidas de conflicto colectivo. Se trata de preservar el mantenimiento de servicios públicos de carácter esencial. En España, el 4 de Diciembre de 2010, se declaró por primera vez en la historia democrática de España, por razón del cierre del espacio aéreo español, debido al abandono de los controladores civiles de tránsito aéreo de sus obligaciones. Duró cuarenta y tres días, y las críticas se sucedieron, entorno a la legitimidad de la decisión tomada por el Gobierno: "Las circunstancias extraordinarias que concurren por el cierre del espacio aéreo español como consecuencia de la situación desencadenada por el abandono de sus obligaciones por parte de los controladores civiles de tránsito aéreo, impiden el ejercicio del derecho fundamental mencionado y determinan la paralización de un servicio público esencial para la sociedad como lo es el servicio de transporte aéreo. Todo ello constituye, sin duda, una calamidad pública de enorme magnitud por el muy elevado número de ciudadanos afectados, la entidad de los derechos conculcados y la gravedad de los perjuicios causados. Para recuperar la normalidad en la prestación del citado servicio público y restablecer los derechos fundamentales de los ciudadanos, hoy menoscabados, y habiendo fracasado todos los intentos para poner fin a la situación de catástrofe pública existente, es indispensable proceder a la declaración del Estado de Alarma en orden a eliminar los obstáculos que impiden su segura y continuada prestación". Real Decreto 1673/2010, de 4 de diciembre, por el que se declara el estado de alarma para la normalización del servicio público esencial del transporte aéreo. BOE nº 295. Disponible en: http://www.boe.es/boe/dias/2010/12/04-2/pdfs/BOE-A-2010-18683.pdf El Estado de Alarma se mantuvo durante cuarenta y tres días y, finalmente, el día 15 de Enero de 2011 se publicó en el BOE el Real Decreto que desmilitarizó el control del tránsito aéreo, por cuanto se consideraba que habían cesado las circunstancias extraordinarias que determinaron la necesidad de encomendar transitoriamente al Ministerio de Defensa las facultades de control de tránsito aéreo atribuidas a la entidad pública empresarial AENA.

[403] Peral, E.V., "Estados de alarma, excepción y sitio"… Op. Cit. p. 159, citando a Mateu-Ros y Martín Retortillo: "No se contiene en este precepto un concepto de orden público, sino una declaración de un orden público enmarcado en un Estado Social y Democrático de Derecho, artículo 1.1 de la Constitución. Así mientras que en la Ley de Orden Público de 31 de julio de 1959 se entendía éste como el normal funcionamiento de las instituciones públicas y privadas, el mantenimiento de la paz interna y el libre y pacífico ejercicio de los derechos individuales, políticos y sociales; hoy el acento se pone en las libertades que encabezan el precepto, porque si bien el orden público es el fundamento de la actividad de policía, entendida como actividad limitadora de los derechos individuales para lograr la convivencia pacífica; no puede concebirse el orden y libertad como ideas en conflicto, ni ampliar exageradamente el concepto de orden público en detrimento de las libertades. La LODES propugna una concepción democrática de orden público en donde es esencial el armonioso juego de las libertades y el libre ejercicio de los derecho individuales reconocidos por las leyes. Los derechos y libertades son la regla, y la excepción su limitación, según el sistema seguido por el artículo 116 de la Constitución y por la LODES. En el marco de nuestro Estado se busca una concepción del orden público acorde con los principios fundamentadores de la Constitución, y que lo considere, por tanto, más como protección del ciudadano que como restricción de libertades. De esta forma, frente al concepto tradicional del orden público que lo equiparaba con el

expresamente la posibilidad de que el Gobierno pueda solicitar la suspensión de derechos constitucionalmente reconocidos, en concreto, los derechos reconocidos en el artículo 17, el derecho a la libertad personal y a la seguridad[404]; en el artículo 18, del apartado 2, el derecho a la inviolabilidad del domicilio, y del apartado 3, el derecho al secreto de las comunicaciones; en el artículo 19, el derecho a elegir libremente su residencia y a circular por el territorio nacional; en el artículo 20, del apartado 1. a., el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones, y del apartado 1. d., el derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión, y del apartado 5, el secuestro de publicaciones, grabaciones y otros medios de información; en el artículo 21, el derecho de reunión; en el artículo 28, del apartado 2, el derecho a la huelga, y finalmente, en el artículo 37, del apartado 2, el derecho de los trabajadores y empresarios a adoptar medidas de conflicto colectivo[405]. Este es un listado tasado y, en ningún caso podrá suponer "un cheque en blanco a la actuación de la Administración, sino que, por una parte, su actuación debe afectar exclusivamente al derecho suspendido y por otra, debe utilizar estas facultades extraordinarias sólo en aquello que sea necesario para la restauración del orden público alterado y únicamente con esta finalidad"[406]. Simplemente pueden ser suspendidos si se acuerda la declaración del Estado de Excepción, en los términos previstos en la Constitución y, por un tiempo limitado, que viene marcado por el artículo 116.3 de la Constitución y se trata de un plazo que no podrá exceder de 30 días, prorrogables por otro plazo igual, con los mismos requisitos.

---

mantenimiento de la paz pública, concepto latente en las leyes de 1933 y 1959, actualmente se identifica el orden público con el mantenimiento de una serie de principios propios de un estado de derecho".

[404] Aunque si bien la Autoridad Gubernativa puede detener a cualquier persona si lo considera necesario para la conservación del orden, siempre que existan fundadas sospechas de que dicha persona vaya a provocar alteraciones del orden público, en el estado de excepción no podrá ser suspendido el derecho que tiene toda persona detenida, a ser informada de forma inmediata, y de modo que le sea comprensible, de sus derechos y de las razones de su detención, no pudiendo ser obligada a declarar. Se garantiza la asistencia de abogado al detenido en las diligencias policiales y judiciales, en los términos que la Ley establezca. Artículos 17.3 y, 55.1 de la CE.

[405] Así lo recoge la Ley Orgánica 4/1981, de 1 de junio, específicamente en los artículos 16 a 23.

[406] Peral, E.V., "Estados de alarma, excepción y sitio"… Op. Cit. p. 165, citando a Berdugo Gómez de la Torre.

Y, por último, respecto al Estado de Sitio[407], el artículo 32 de la la Ley Orgánica 4/1981, de 1 de junio, establece que el Gobierno podrá proponer al Congreso de los Diputados la declaración de Estado de Sitio "cuando se produzca, o amenace producirse, una insurrección o acto de fuerza contra la soberanía o independencia de España, se integridad territorial o el Ordenamiento Constitucional, que no pueda resolverse por otros medios", situaciones en las que ya no se trata de restablecer meramente el orden público, sino la paz en todo el territorio nacional[408], atribuyendo a las autoridades militares competencias que hasta ahora correspondían a autoridades civiles, pero sometidos siempre en la ejecución de éstas al Gobierno[409]. En esta situación, se podrá incluso decretar la suspensión temporal de garantías jurídicas del detenido, por ejemplo, el derecho a ser informado de forma inmediata y comprensible de sus derechos y de las razones de su detención, en el momento de ser detenido[410].

En la materia que nos ocupa, en el caso de suspensión del derecho fundamental al secreto de las comunicaciones, tanto para el Estado de Excepción como para el Estado de Sitio, será la extraordinaria gravedad de las situación en que se encuentre el país, la que justifique o no la decisión de adoptar esta medida. Pero no se ha dejado al arbitrio de las autoridades la intervención de todo tipo de comunicaciones, sino que se determinarán al amparo de la excepcionalidad de las circunstancias y con el único fin de

---

[407] Artículo 33 de la Ley Orgánica 4/1981, de 1 de junio: "En virtud de la declaración del Estado de Sitio, el Gobierno, que dirige la Política Militar y de la Defensa, de acuerdo con el artículo 97 de la Constitución, asumirá todas las facultades extraordinarias previstas en la misma y en la presente Ley. A efectos de lo dispuesto en el párrafo anterior, el Gobierno designará la autoridad militar que, bajo su dirección, haya de ejecutar las medidas que procedan en el territorio a que el Estado de Sitio se refiera".
Artículo 36. "Las autoridades civiles continuarán en el ejercicio de las facultades que no hayan sido conferidas a la autoridad militar de acuerdo con la presente Ley. Aquellas autoridades darán a la militar las informaciones que esta le solicite y cuantas noticias referentes al orden público lleguen a su conocimiento".

[408] Peral, E.V., "Estados de alarma, excepción y sitio"… Op. Cit. p. 176, citando a Fernández Segado: "Los orígenes del estado de sitio se encuentran en la diferenciación entre el estado de sitio militar, régimen legal por el que se debía regir toda plaza militar o fortificación de igual índole sometida a una amenaza de guerra; y estado de sitio político, en donde se autoriza la declaración del estado de guerra a los municipios en el interior del país y, asimismo, prevé el que tales municipios deban encontrarse en estado de guerra en todas aquellas circunstancias a que se refiere la propia ley".

[409] "La institución del estado de sitio se caracteriza por entrañar un régimen de policía excepcional, justificado por la idea de peligro nacional". FERNANDEZ RODERA, J.A. "Las Fuerzas Armadas y el estado de sitio", en *Libertades públicas y Fuerzas Armadas: actas de las Jornadas de estudio celebradas en el Instituto de Derechos Humanos de la Universidad Complutense*. Madrid, 1984. p. 183.

[410] Aunque en todo caso habrán de respetarse las garantías previstas por el apartado 6 del artículo 116 de la CE: "La declaración de los estados de alarma, de excepción y de sitio no modificará el principio de responsabilidad del Gobierno y de sus agentes reconocidos en la Constitución y en las Leyes".

facilitar las tareas de las autoridades en el reestablecimiento del orden público.

En el primer Proyecto de la Ley reguladora del Estado de Alarma, de Excepción y de Sitio, era el denominado "Ley de Seguridad Ciudadana", del que sólo el Capítulo III se refería a "Los estados de alarma, excepción y sitio"[411].

En dicho proyecto el artículo 33 decía inicialmente que "La autoridad gubernativa podrá intervenir y controlar, cuando lo considere necesario, toda clase de transportes y comunicaciones, incluidas las postales, telegráficas y telefónicas"[412].

Pero los debates llevaron a introducir en forma de enmiendas una serie de modificaciones que llevarían a la redacción actual, pasando a ser el artículo 18[413]. En concreto, la enmienda nº 245, presentada por el grupo socialista del Congreso de los Diputados, dio una mayor definición a los límites que exigía el artículo 18 de la CE, y se propuso la siguiente redacción:

1. "Si suspendiera el artículo 18.3 de la Constitución, la autoridad gubernativa podrá intervenir las comunicaciones postales telegráficas y telefónicas si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos.

2. De la intervención decretada se dará cuenta inmediata al juez competente, quien podrá controlar y determina la forma en que dicha intervención debe efectuarse".

[411] La Ponencia, primero, y la Comisión de Constitución, después, aprobaron la enmienda núm. 98 del Grupo parlamentario Comunista, de forma que el Proyecto de Ley se dividió en cuatro proyectos distintos, entre los que se encontraba el de los estados de alarma, excepción y sitio. Diario de sesiones del Congreso de los Diputados, Sesión plenaria nº 160, celebrada el 21 de Abril de 1981. p. 9875. Presentación del proyecto. Disponible en: http://www.congreso.es/public_oficiales/L1/CONG/DS/PL/PL_160.PDF

[412] Boletín Oficial de las Cortes Generales 21 de Septiembre de 1979. Disponible en: http://www.congreso.es/public_oficiales/L1/CONG/BOCG/A/A_073-I.PDF

[413] Boletín Oficial de las Cortes Generales 14 de Abril de 1981. Disponible en: http://www.congreso.es/public_oficiales/L1/CONG/BOCG/A/A_073-I-T.PDF

Otra aportación significativa, en este mismo sentido, fue la del Grupo Vasco, la enmienda nº 74, que propuso añadir un párrafo diciendo que: "De las observaciones postales, telegráficas y telefónicas deberá dar cuenta la autoridad gubernativa a la judicial". Pero la propuesta más radical, fue la introducida por el Grupo Mixto, por D. Juan María Bandrés Molet, en las enmiendas nº 33 a 41, en las que planteaba directamente la supresión de aquel artículo 33, porque la Constitución determina que una "ley orgánica regulará los estados de alarma, excepción y de sitio y las competencias y limitaciones correspondientes" (artículo 116). En el artículo 55, apartado 1, de la Constitución se dice que "los derechos reconocidos en los artículos… podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio…" Pero no es una obligación legal, sino una posibilidad que con esta ley se agota al máximo. Los artículos 33, 35, 36 y 37, apartado 3, pueden utilizarse perfectamente por razones ideológico-político".

Finalmente, se aceptaron las enmiendas relativas a la preceptiva notificación al juez competente de la intervención decretada, y para aquellas situaciones excepcionales, dicho precepto legal quedó redactado como sigue:

> "Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo 18.3, de la Constitución, la Autoridad Gubernativa podrá intervenir toda clase de comunicaciones, incluidas las postales, telegráficas y telefónicas. Dicha intervención solo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público.
>
> Dos. La intervención decretada será comunicada inmediatamente por escrito motivado al juez competente".

2.- Fuerzas y Cuerpos de Seguridad del Estado; ficheros de datos.

La Constitución Española prevé la base jurídica de las Fuerzas y Cuerpos de Seguridad en el artículo 104, y lo hace de forma separada de las Fuerzas Armadas (artículo 8), tratándolas como dos instituciones distintas y remitiéndose a sus respectivas Leyes Orgánicas para el desarrollo de sus competencias y límites de actuación.

Las Fuerzas y Cuerpos de Seguridad del Estado tienen como objetivo principal "proteger el libre ejercicio de los derechos libertades y garantizar la seguridad ciudadana y, las Fuerzas Armadas tienen el deber de garantizar la soberanía e independencia de España, defender su integridad territorial y el ordenamiento constitucional", así, el mantenimiento de la "seguridad pública" constituye un verdadero servicio público cuyo titular exclusivo es el Estado[414], y también las Comunidades Autónomas y las Corporaciones Locales deberán contribuir prestando el correspondiente auxilio, según lo dispuesto por sus Estatutos de Autonomía y, la Ley Reguladora de las Bases de Régimen Local, en el marco de lo dispuesto en la propia Ley Orgánica 2/1986.

Por tanto, se considera que son Fuerzas y Cuerpos de Seguridad las del Estado dependientes del Gobierno de la Nación, así como los Cuerpos de Policía dependientes de las Comunidades Autónomas (Andalucía, Valencia, Galicia, País Vasco, Navarra y Cataluña), y de las Corporaciones Locales, cuya Ley Orgánica regula sus principios básicos de acción: actuar con respeto al ordenamiento jurídico, con neutralidad, integridad y dignidad, así como con sometimiento a los principios de jerarquía y subordinación, entre otros.

[414] Artículo 1.1 de la Ley Orgánica 2/1986, de 13 de Marzo, de Fuerzas y Cuerpos de Seguridad y, artículo 149.1.29ª de la Constitución.

El preámbulo de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, afirma "que los principios básicos de actuación de las Fuerzas y Cuerpos de Seguridad son los ejes fundamentales, en torno a los cuales gira el desarrollo de las funciones policiales, derivando a su vez de principios constitucionales más generales, como el de legalidad o adecuación al Ordenamiento jurídico, (...) como emanación del principio constitucional de igualdad ante la Ley, le exigen la neutralidad política, la imparcialidad y la evitación de cualquier actuación arbitraria o discriminatoria por encima de cualquier otra finalidad, la Ley pretende ser el inicio de una nueva etapa en la que destaque la consideración de la policía como un servicio público dirigido a la protección de la comunidad, mediante la defensa del Ordenamiento Democrático".

Junto a esta norma general, otras de rango inferior contribuyen a precisar las pautas de actuación de las Fuerzas y Cuerpos de Seguridad, por ejemplo la Ley 23/1992, de 30 de julio, de Seguridad Privada, la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de video cámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos o, la Ley 42/1999, de 25 de noviembre, de Régimen de Personal de la Guardia Civil. Si bien, son la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad y, la Ley Orgánica 1/1992, de 21 de febrero, de Protección de la Seguridad Ciudadana, las más destacadas.

Las tareas de las Fuerzas y Cuerpos de Seguridad están sujetas a todas las garantías legales y constitucionales del Estado de Derecho, y deben hacer su trabajo con respeto a los valores y derechos que éste consagra. Explica al respecto el Tribunal Constitucional que "de la Constitución se deduce que las Fuerzas de Policía están al servicio de la comunidad para garantizar al ciudadano el libre y pacífico ejercicio de los derechos que la Constitución y la Ley les reconocen, y este es el sentido de artículo 104.1 C.E. que puede considerarse directamente heredero del artículo 12 de la Declaración de Derechos del Hombre y del Ciudadano, configurando a la Policía como un servicio público para la comunidad, especializado en la prevención y lucha contra la criminalidad, el mantenimiento del orden y la seguridad pública y la protección del libre

ejercicio de los derechos y libertades. El artículo 104.1 C.E. trata de asegurar la adaptación del sistema policial, de sus funciones y de sus principios básicos al orden constitucional, subrayando, en un plano positivo, y en la misma línea que el artículo 53 C.E., la función de garantía de libertades y derechos fundamentales que también corresponde a la Policía pero, al mismo tiempo, negativamente destacando que la actuación de la fuerza de la Policía debe respetar también y garantizar las libertades y derechos fundamentales del ciudadano.

El artículo 104.1 C.E. refleja un necesario y no siempre fácil equilibrio en relación con la actuación de las fuerzas de la Policía, que son un instrumento necesario para asegurar la libertad y la seguridad de los ciudadanos, pero que, al mismo tiempo, por la posibilidad de uso legítimo de la fuerza y de medidas de, coacción supone, en el caso de extralimitaciones, una puesta en peligro de la libertad y seguridad de aquellos, así como de otros derechos y bienes constitucionales de la persona (vida, integridad física, intimidad, inviolabilidad del domicilio, etc.). Un orden constitucional democrático es incompatible con el uso de métodos represivos ilegítimos y por ello mismo exige una protección adecuada del ciudadano frente al peligro de eventuales extralimitaciones, lo que incluye también la posibilidad de acudir a la vía judicial para reaccionar frente a los excesos y abusos, con trascendencia penal, por parte de los miembros de las Fuerzas y Cuerpos de Seguridad, en el uso, en principio legítimo, de la fuerza y de los medios de coacción.

El legislador ha de ponderar, por tanto, los valores constitucionales en juego, de modo que la protección de los medios de actuación de las Fuerzas de Policía no puede suponer un sacrificio de bienes y derechos constitucionales y del propio respeto del Estado de Derecho, ni una limitación efectiva de la posibilidad de verificar judicialmente los abusos o extralimitaciones, por excepcionales que puedan ser, en que eventualmente incurran los miembros de las Fuerzas de Policía en el ejercicio de sus funciones"[415].

[415] Sentencia del Tribunal Constitucional nº 55/1990, de 28 de Marzo de 1990. (F.Jº.5º).

Y entre esos medios de actuación se encuentra, con un papel cardinal, la tecnología. Su desarrollo permite actualmente usar técnicas de investigación y detección de delitos, pero que de no ser empleadas con límites, podrían provocar la restricción de derechos fundamentales de los ciudadanos hasta el punto de hacerlos irreparables. La tecnología todo lo puede, y la "seguridad" no debe ser su carta blanca.

2.1.- El tratamiento de datos al servicio de la Policía.

La protección de la persona, frente a las posibilidades que ofrece la tecnología para tratar la información que le concierne, sea o no íntima, para tratar sus datos personales en perfiles perfectamente individualizados, ha de tener previstas normativamente una serie de garantías, tanto previas como posteriores al tratamiento, a las que pueda acogerse en caso de ver sus derechos vulnerados de forma ilícita.

Decía la Memoria de la Agencia Española de Protección de Datos de 1995 que "la naturaleza de los datos personales almacenados o tratados con fines policiales, así como la propia inclusión de datos en un fichero policial, hacen de éstos ficheros una amenaza potencial particularmente grave para el honor e intimidad de los ciudadanos, considerándose por ello prioritario el control de sus condiciones de utilización, especialmente en los casos en que dichos ficheros incluyen alguno de los denominados datos sensibles", y tras los graves acontecimientos terroristas vividos en EEUU (2001), España (2004) y Londres (2005), parece que la expresión "para salvaguarda de la seguridad" sea carta blanca para permitir todo tipo tratamiento de datos personales por la autoridad policial, sin embargo, nada más lejos, pues además de las leyes, el poder judicial tiene la capacidad y el deber de supervisar toda operación que implique la restricción de cualesquiera

derechos constitucionales cuando tenga conocimiento de ello. Por ejemplo, la videovigilancia, la utilización de datos biométricos y datos genéticos, el uso del RFID en seres humanos, la recogida de datos de los pasajeros transfroterizos, la conservación de los datos de tráfico por las operadoras o la interceptación de las comunicaciones, etc., son cuestiones que vienen siendo debatidas en el estudio de la influencia real de las tecnologías en la vida de cada persona y, en general, de su posible influencia en el comportamiento de la sociedad.

Precisamente, en una comparecencia ante la Comisión Constitucional del Congreso de los Diputados[416], el entonces Director de la Agencia de Protección de Datos, JOSE LUIS PIÑAR MAÑAS quiso poner de manifiesto que "vivimos momentos en los que se está produciendo una tensión creciente entre la protección de datos personales y el derecho de todos los ciudadanos a que su seguridad esté garantizada. El golpe que las atrocidades terroristas provoca no sólo en las víctimas sino en el conjunto de la sociedad, es lo que caracteriza a los delitos de terrorismo frente a otras formas de delincuencia y si su consecuencia es la supresión o restricción de los derechos fundamentales, el objetivo de este crimen estará plenamente alcanzado*".* Y en este sentido explicaba que las sociedades democráticas disponen hoy en día de suficientes medios, "flexibles y ágiles, que permiten luchar contra el terrorismo sin menoscabo de los derechos fundamentales".

En la necesidad de garantizar especialmente el derecho fundamental a la protección de datos, el uso correcto de la información personal de los individuos por parte de las autoridades gubernativas, se debe buscar una fórmula equilibrada con las crecientes necesidades de seguridad. PIÑAR MAÑAS quiso llamar la atención además sobre los aspectos que en ese momento, incluso aún hoy, preocupaban de forma especial: "la obligación de retención de datos de tráfico, en el ámbito de las comunicaciones electrónicas y, en menor medida, en el tratamiento de datos

[416] Comparecencia del Señor Director de la Agencia Española de Protección de Datos, para informar sobre la memoria de la Agencia Española de Protección de Datos correspondiente al año 2004 (a petición propia).Nº de Expediente 212/674, celebrada el miércoles 28 de Septiembre de 2005, ante la Comisión Constitucional. Sesión nº 10. Diario de Sesiones del Congreso de los Diputados, nº 353.

biométricos en documentos de identificación de los ciudadanos, como son el documento nacional de identidad y el pasaporte".

Esta intervención tuvo respuesta de algunos de los parlamentarios presentes, en la misma línea de preocupación. LUIS MARDONES SEVILLA, Diputado por Coalición Canaria, refirió la posibilidad de que al margen de que el coste económico de la implantación de esas medidas tecnológicas fuese caro, lo que realmente le preocupaba es que "sea caro en la democracia, en el régimen de libertades, y lo plasmó de forma contundente diciendo que por supuesto que estamos en contra del terrorismo, de las mafias y de los delitos organizados en cualquier aspecto de la criminalidad, pero vamos a mantener democráticamente lo que tanto nos ha costado aquí. A ver si la brigada político social va a ser sustituida ahora en este país por una serie de instrumentos de conocimiento interno, de la radiografía (...). Vamos a poner pie en pared y vamos a saber qué garantías constitucionales tiene esto*".*

El Director de la Agencia, respondía ante estas afirmaciones que ciertamente "no es posible descuidar el pleno y absoluto respeto a los derechos fundamentales. La gran victoria de los terroristas sería acabar con la democracia, y este es un planteamiento que no admite ningún género de dudas ni de posiciones intermedias (...) Es posible adoptar medidas de lucha contra el terrorismo y de lucha contra la delincuencia organizada sin menoscabar el derecho fundamental a la protección de datos y sin que resulte caro para la democracia*".*

Estas preocupaciones sobre el control de la lucha antiterrorista, por que sea llevada a cabo siempre en un marco de respeto de libertades de los ciudadanos, son herencia también del debate europeo, del artículo K.3 del Tratado de la Unión Europea[417], en el que el Consejo de la Unión Europea

[417] Disposiciones relativas a la cooperación en los ámbitos de la justicia y de los asuntos de interior, en las que se señala que el Consejo Europeo podrá, a iniciativa de cualquier Estado Miembro, "celebrar convenios recomendando su adopción a los Estados miembros según sus respectivas normas constitucionales" en materia de cooperación judicial en materia penal; de cooperación aduanera y, de "cooperación policial para la prevención y la lucha contra el terrorismo, el tráfico ilícito de drogas y otras formas graves de delincuencia internacional, incluidos, si es necesario, determinados aspectos de la cooperación aduanera en conexión con la organización, a escala de la Unión, de un sistema de intercambios de información dentro de una Oficina Europea de Policía (Europol)".

recomendaba en el año 1995, en su Acto 95/C 316/01, de 26 de Julio, adoptar un Convenio por el que se crearía la Oficina Europea de Policía (Convenio Europol), establecida en la Haya.

El Convenio Europol, tenía como objetivo crear una institución coordinada para procurar la cooperación policial en Europa, entre los Estados miembros, para luchar contra el terrorismo, el tráfico ilícito de drogas y demás formas graves de delincuencia organizada internacional, aunque careciese de poderes ejecutivos como los de los servicios de policía de los Estados miembros[418], no pudiendo detener a individuos, ni registrar domicilios. Aún así, el flujo de datos es la base de su actividad, en coordinación con las unidades nacionales de cada Estado miembro y, Europol es en Europa el organismo con mayores atribuciones para el uso de todo tipo de tecnología en la realización de sus tareas, dado que esencialmente se encarga de facilitar el intercambio de información entre los Estados miembros, en materia de la prevención y la lucha contra el terrorismo; el tráfico de drogas; el tráfico de seres humanos; las redes de inmigración clandestina; el tráfico ilícito de materias radiactivas y nucleares; el tráfico de vehículos robados; la lucha contra la acuñación de monedas falsas y la falsificación de medios de pago; el blanqueo de dinero (excepto infracciones primarias).

Pues bien, teniendo en cuenta las ilimitadas posibilidades del tratamiento de información con la tecnología actual, el propio Convenio, consciente de esto, se preocupaba de incluir límites y precauciones a tener

[418] Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía (Convenio Europol), hecho en Bruselas el 26 de julio de 1995. Artículo 2. 1. Objetivo. "El objetivo de Europol consiste en mejorar, en el marco de la cooperación policial entre los Estados miembros acorde con el Tratado de la Unión Europea y merced a las medidas que se enumeran en el presente Convenio, la eficacia de los servicios competentes de los Estados miembros y la cooperación entre ellos, para prevenir y luchar contra las formas graves de delincuencia internacional, cuando existan indicios concretos o motivos razonables para creer que haya implicada una estructura delictiva organizada y que dos o más Estados miembros se vean afectados de tal modo que, debido al alcance, gravedad y consecuencias de los actos delictivos, se requiera una actuación común de los Estados miembros. A efectos del presente Convenio, las siguientes formas de delincuencia deben considerarse formas graves de delincuencia internacional: los delitos cometidos o que puedan cometerse como actividades de terrorismo que atenten contra la vida, la integridad física y la libertad de las personas, así como contra sus bienes, el tráfico ilícito de estupefacientes, las actividades ilícitas de blanqueo de dinero, el tráfico de material nuclear y radiactivo, las redes de inmigración clandestina, la trata de seres humanos y el tráfico de vehículos robados, así como las formas de delincuencia establecidas en el Anexo o las manifestaciones específicas de la misma".

en cuenta en favor de la protección de los derechos de las personas que pudieran verse afectadas por la actividad policial.

Por ejemplo, según el artículo 6 del Convenio, el sistema informatizado de recogida de datos que utiliza Europol, "no deberá en ningún caso conectarse a otros sistemas de tratamiento automatizado, exceptuado el sistema de tratamiento automatizado de las unidades nacionales y, en todo caso: se establecerá una autoridad común de control independiente cuyo cometido será vigilar la actividad de Europol, con arreglo a lo dispuesto en el presente Convenio, con el objeto de garantizar que el almacenamiento, el tratamiento y la utilización de los datos de que dispongan los servicios de Europol no vulneren los derechos de las personas. La autoridad común de control controlará, además, la licitud de la transmisión de datos que procedan de Europol" (artículo 24). Esta Autoridad de Control también es controlada en su actividad, pues ha de elaborar informes de actividad que se remitirán periódicamente al Parlamento Europeo y al Consejo.

En materia de protección de datos de carácter personal, el Convenio recoge expresamente unos requisitos mínimos que deben cumplir todos los Estados firmantes del mismo. Prevé por ejemplo un plazo máximo de tres años de conservación de los datos (artículo 22) y, exige que Europol tome las medidas técnicas y organizativas necesarias para la ejecución del Convenio (artículo 25), que se considerarán necesarias, siempre y cuando el coste que suponga adoptarlas guarde relación con el objetivo de protección que se persiga.

Cada Estado miembro y Europol, acordarán por ejemplo las medidas más adecuadas para impedir que cualquier persona no autorizada acceda a las instalaciones utilizadas para el tratamiento de datos personales (control de entrada a las instalaciones); para impedir que los soportes de datos puedan ser leídos, copiados, modificados o retirados por personas no autorizadas (control de los soportes de datos); para impedir que se introduzcan sin autorización en los ficheros, o que puedan conocerse, modificarse o suprimirse sin autorización datos personales almacenados

(control de almacenamiento); para impedir que los sistemas de tratamiento automatizado de datos puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos (control de la utilización); para garantizar que las personas autorizadas para el uso de un sistema de tratamiento automatizado de datos sólo puedan tener acceso a los datos que sean de su competencia (control del acceso); para garantizar que pueda verificarse y constatarse a qué órganos pueden transmitirse datos personales a través de las instalaciones de transmisión de datos (control de la transmisión); para garantizar que pueda comprobarse y constatarse a posteriori qué datos personales se han introducido en los sistemas de tratamiento automatizado de datos, en qué momento y por quién (control de la introducción); para impedir que, en el momento de la transmisión de datos personales y durante el transporte de soportes de datos, los datos puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte); para garantizar que los sistemas utilizados puedan repararse rápidamente en caso de avería (restablecimiento) y, para garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados inmediatamente (fiabilidad), y que los datos almacenados no sean falseados por defectos de funcionamiento del sistema (autenticidad).

En general, las competencias de este organismo se centran en el control de la licitud de los tratamientos de datos personales y en la tutela de los derechos de las personas, dado que se prevé un precepto sobre la responsabilidad en materia de protección de datos (artículo 15), los niveles de protección a aplicar según la naturaleza del dato (artículo 14) y, en especial, sobre la rectificación y supresión de los datos erróneos (artículo 20) y, el derecho de acceso (artículo 19), sobre el que se prevé que "cualquier persona que desee ejercer su derecho de acceso a la información, que le afecte, almacenada en Europol o hacer que se verifique esa información podrá dirigir gratuitamente una solicitud en ese sentido, en el Estado miembro de su elección, a la autoridad nacional competente, que deberá comunicarlo sin dilación a Europol y avisar al solicitante de que Europol le responderá directamente".

Otro convenio Europeo relevante, en cuanto a la investigación policial del terrorismo y, el control del debido respeto a la protección de datos personales, es el Convenio Schengen.

El 14 de junio de 1985, se firmó en Bonn el Acuerdo de Schengen, entre Alemania, Bélgica, Francia, Luxemburgo y los Países Bajos, con el objetivo de eliminar progresivamente los controles en las fronteras comunes y establecer un régimen de libre circulación para todos los nacionales de los Estados firmantes. Más adelante este acuerdo fue completado para su aplicación, con un convenio, el Convenio de Schengen, firmado el 19 de junio de 1990 por los mismos Estados miembros (aunque no entró en vigor hasta 1995), para definir las condiciones y las garantías de aplicación de la libre circulación. Ambos pactos, junto con otros acuerdos conexos y la normativa derivada de ello, conformó lo que se dio en llamar el "acervo Schengen", que fue incorporado al marco jurídico de la Unión Europea mediante un protocolo anexo al Tratado de Ámsterdam de 1999.

En la puesta en práctica de los objetivos de estos compromisos, para conseguir la generación de un espacio sin fronteras, se necesitaba la creación de un sistema de información que facilitase la prevención y persecución de los delitos y que mantuviese en definitiva la seguridad de los Estados miembros implicados: el Sistema de Información Schengen (SIS), que permitiría que "las autoridades designadas de las Partes contratantes, mediante un procedimiento de consulta automatizado, dispongan de descripciones de personas y de objetos, al efectuar controles en la frontera y comprobaciones y otros controles de policía y de aduanas realizados dentro del país de conformidad con el derecho nacional" [419], y su objetivo no es otro que "preservar el orden y la seguridad públicos, incluida la seguridad del Estado, y la aplicación de las disposiciones del presente Convenio sobre la circulación de personas por los territorios de las Partes contratantes, con la ayuda de la información transmitida por dicho Sistema" (artículo 93).

[419] Artículo 92 del Convenio de aplicación del Acuerdo Schengen, de 14 de Junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal Alemana y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes.

Las previsiones relativas a la protección de la información que puede ser tratada e intercambiada, se recogen en los artículos 93 a 117 del Convenio, y de ellos destaca la preocupación por limitar la recogida de datos a tan sólo determinadas categorías, como el nombre y apellidos, la fecha y lugar de nacimiento, la nacionalidad, el sexo, el motivo de la inscripción, etc. (artículo 94); por restringir el acceso a dicha información, exclusivamente a las autoridades competentes para los controles fronterizos y las comprobaciones de policía y de aduanas realizadas dentro del país, así como para la coordinación de las mismas (artículo 101); por limitar las finalidades para las que se pueden utilizar los datos registrados (artículo 102) y, por establecer severos controles de admisibilidad de las consultas que se pueden realizar (artículo 103).

Por otra parte, el Convenio también prevé disposiciones relativas al ejercicio de los derechos de las personas (artículos 109 y 110), especialmente los derechos de rectificación y de cancelación para los casos de informaciones erróneas o inexactas, y el derecho de acceso, "el derecho de toda persona a acceder a los datos que se refieran a ella y estén introducidos en el Sistema de Información de Schengen se ejercerá respetando el Derecho de la Parte contratante ante la que se hubiere alegado tal derecho". Pero también prevé límites al ejercicio de los mismos, por ejemplo, se dice que "no se facilitará información a la persona de que se trate si dicha información pudiera ser perjudicial para la ejecución de la tarea legal consignada en la descripción o para la protección de los derechos y libertades de terceros. Se denegará en todos los casos durante el período de descripción con vistas a una vigilancia discreta".

La Autoridad de Control común, prevista en el artículo 115, será la encargada del control de la unidad de apoyo técnico del Sistema de Información de Schengen, comprobando que el tratamiento y la utilización de los datos introducidos en el SIS no atentan contra los derechos de la persona de que se trate.

En la misma línea del Convenio Europol, Schengen hace referencia al compromiso de las partes del Convenio (artículo 118) a adoptar las

medidas adecuadas para impedir que toda persona no autorizada acceda a las instalaciones utilizadas para el tratamiento de datos de carácter personal (control en la entrada de las instalaciones); para impedir que los soportes de datos puedan ser leídos, copiados, modificados o retirados por una persona no autorizada (control de los soportes de datos); para impedir que se introduzcan sin autorización en el fichero o que puedan conocerse, modificarse o suprimirse sin autorización datos de carácter personal introducidos (control de la introducción); para impedir que los sistemas de tratamiento automatizado de datos puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos (control de la utilización); para garantizar que, para el uso de un sistema de tratamiento automatizado de datos, las personas autorizadas sólo puedan tener acceso a los datos que sean de su competencia (control del acceso); para garantizar la posibilidad de verificar y comprobar a qué autoridades pueden ser remitidos datos de carácter personal a través de las instalaciones de transmisión de datos (control de la transmisión); para garantizar que pueda verificarse y comprobarse a posteriori qué datos de carácter personal se han introducido en el sistema de tratamiento automatizado de datos, en qué momento y por qué persona han sido introducidos (control de la introducción); para impedir que, en el momento de la transmisión de datos de carácter personal y durante el transporte de soportes de datos, los datos puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte). En especial exige que cada parte contratante adopte "medidas especiales para garantizar la seguridad de los datos durante la transmisión de datos a servicios situados fuera del territorio de las Partes contratantes".

Por último, es necesario hacer mención especial a las Decisiones Marco adoptadas en el seno de la UE, en materia de protección de datos y seguridad policial.

El Tratado de la Unión Europea recogía el compromiso de la colaboración policial entre los Estados miembros, en el que se llamaba III Pilar de la Unión Europea, invitando a la aplicación del Derecho nacional de cada Estado en estas materias y, a la cooperación intergubernamental. No

existen reglas armonizadas en el nivel europeo y, en todo momento rigen las normativas nacionales en materia de derecho penal, así como aquellas normas que puedan afectar a la protección de datos en este ámbito específico. Sin embargo, si que hay un nivel básico común en la legislación de protección de datos de los Estados miembros, basado en el "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" (o Convenio 1084), que se aplica a todos los tratamientos de datos llevados a cabo por las fuerzas y cuerpos de seguridad, como por ejemplo, el que recoge la Recomendación (87) 15, aprobada por el Consejo de Ministros del Consejo de Europa, por la que se regula el uso de datos personales en el ámbito policial, que se ha incorporado como norma de mínimos en varios convenios y decisiones de la UE como Schengen, Europol, Sistema de Información Aduanera o Eurojust, y que se articula en torno a ocho principios: "Control y Notificación"; "Recogida de datos"; "Almacenamiento de datos"; "Uso de los datos por parte de la policía"; "Cesiones de datos"; "Publicidad y Derechos de las personas"; "Duración del almacenamiento y Actualización de los datos"; y "Seguridad de los datos".

La base para una cooperación policial coordinada se encuentra en el conocido como "Principio de Disponibilidad". El Programa de La Haya[420], adoptado en el Consejo Europeo del 4 y 5 de noviembre de 2004, recogía los propósitos de la UE para reforzar el Espacio de Libertad, Seguridad y Justicia y, en este sentido, para mejorar concretamente la cooperación en la lucha contra el terrorismo y el crimen organizado definía este principio señalando que: "En todo el territorio de la Unión, un funcionario de policía de un Estado miembro que necesite información para llevar a cabo sus obligaciones pueda obtenerla de otro Estado miembro. El organismo policial del otro Estado miembro que posea dicha información la facilitará para el propósito indicado, teniendo en cuenta el requisito de las investigaciones en curso en dicho

[420] Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 10 de mayo de 2005, *Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia* [COM (2005) 184 final – Diario Oficial C 236 de 24.9.2005]. Disponible en: http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/l16002_es.htm

Estado". Es decir, se establece la obligación de cumplir los requerimientos de información del resto de Estados miembros.

La primera experiencia nace con la Decisión Marco 2006/960/JAI del Consejo de 18 de diciembre de 2006 sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea[421], con las condiciones, causas y plazos para suministrar la información entre ellos, aunque se remite en gran parte a las disposiciones nacionales sobre protección de datos de los Estados receptores, afirmando que deben satisfacer, al menos, los estándares del Consejo de Europa. Pero, al imponerse este modelo tan amplio de intercambio de información, las autoridades europeas de protección de datos exigieron un esfuerzo común para garantizar un equilibrio adecuado entre el derecho a la intimidad y la seguridad[422].

El Supervisor Europeo de Protección de Datos elabora varios dictámenes en los que analiza la situación, y aborda la necesitad de dicho equilibrio, así, el Dictamen de 19 de diciembre de 2005, de 29 de noviembre de 2006 y, de 27 de abril de 2007.

La Decisión finalmente aprobada, fue la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos

[421] Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:ES:PDF

[422] "En la Declaración aprobada en la Conferencia Europea de Cracovia en abril de 2005 ya se ponía de manifiesto que "La Conferencia Europea de Autoridades de Protección de Datos de 2005 es consciente de la necesidad de mayor cooperación entre las fuerzas y cuerpos de seguridad, dentro de la UE y con terceros estados. Al mismo tiempo es evidente que el Convenio 108 es demasiado general para salvaguardar efectivamente la protección de datos en el sector policial. Dada la obligación de la Unión de respetar los derechos y libertades fundamentales, las iniciativas como el Principio de Disponibilidad, solo se deberían introducir sobre la base de un sistema adecuado de protección de datos que garantice un estándar alto y equivalente de protección de datos". En la misma declaración se manifestaba la satisfacción de la Conferencia por someter la aplicación del Principio de Disponibilidad a estrictas condiciones de respeto a los principios de protección de datos y se daba la bienvenida a la Propuesta inicial de la Comisión para establecer una Decisión Marco sobre Protección de Datos en el III Pilar. En la Conferencia de Budapest del siguiente año, a través de una nueva Declaración, se insistía en las mismas ideas y finalmente, en la Conferencia celebrada en Chipre en mayo de 2007, cuando la Propuesta inicial de la Comisión ya había sido desechada y los debates se centraban en un texto alternativo en el que se limitada el ámbito de aplicación únicamente a los datos intercambiados entre Estados miembros, la Conferencia expresaba su opinión: "Se reitera el impacto nacional de las iniciativas de la Unión y el claro riesgo de que limitar el alcance a los datos intercambiados haría el campo de aplicación de la Decisión particularmente inseguro e incierto, las Autoridades Europeas de Protección de datos resaltan que solo un alcance comprensivo que cubra todos los tratamientos de datos personales podría ofrecer a las personas la necesaria protección". Emilio Aced Félez "Principio de Disponibilidad y protección de datos en el ámbito policial", en *Noticias Jurídicas*. Abril 2010. Disponible en: http://noticias.juridicas.com/articulos/15-Derecho%20Administrativo/201004-123095321697634.html

personales tratados en el marco de la cooperación policial y judicial en materia penal. Esta norma[423], en síntesis, pretende "proteger los derechos y libertades fundamentales de las personas físicas, cuando sus datos personales son tratados en el marco de la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales y la ejecución de sanciones penales". Recoge una serie de principios por los cuales se entiende que los datos personales obtenidos de otro Estado miembro "serán tratados únicamente para el fin para el cual fueron transmitidos. No obstante, en ciertos casos, podrán ser tratados para otros fines distintos, como son la prevención, la investigación, la detección o el enjuiciamiento de otras infracciones penales, la ejecución de otras sanciones penales o la prevención de amenazas a la seguridad pública. El Estado miembro receptor respetará todas las limitaciones específicas sobre intercambio de datos que estén previstas en la legislación del Estado miembro transmisor". Y para ello, requiere a los Estados miembros que sus autoridades apliquen "las medidas de seguridad necesarias para proteger los datos personales contra cualquier forma de tratamiento ilícito. Esto incluye la pérdida accidental, la alteración o la difusión no autorizada de los datos personales, o el acceso no autorizado a los mismos. En el caso del tratamiento automatizado de los datos, deberán aplicarse medidas específicas. Las autoridades nacionales de control de los Estados miembros se encargarán de vigilar la aplicación de esta Decisión Marco y de prestar asesoramiento sobre la misma. Para que puedan llevar a cabo esta labor, dichas autoridades dispondrán de poderes de investigación, de poderes efectivos de intervención así como de capacidad procesal. Los Estados miembros establecerán sanciones eficaces, proporcionadas y disuasorias, que se impondrán en caso de incumplimiento de las disposiciones de esta Decisión Marco".

En concreto, la Decisión Marco del Consejo 2006/960/JAI, constituyó un instrumento vinculante y decisivo para España, teniendo fiel reflejo legislativo con la Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de

[423] Disponible en:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:ES:PDF
Y síntesis, en:
http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/jl0018_es.htm

los Estados miembros de la Unión Europea[424]. En cumplimiento de los principales objetivos de la Unión Europea en materia de seguridad, para lograr un espacio de libertad, seguridad y justicia, previendo y combatiendo la delincuencia mediante una mayor cooperación entre los servicios de seguridad de los Estados miembros de la Unión Europea (en adelante Estados miembros), respetando al mismo tiempo los principios y las normas sobre derechos humanos, libertades fundamentales y el Estado de Derecho, esta norma es necesaria, para regular el hecho de que "los servicios de seguridad españoles puedan intercambiar información e inteligencia de otros Estados miembros en las distintas fases de la investigación, desde la fase de recogida de inteligencia criminal hasta la fase de investigación criminal". La Ley debe garantizar que "determinada información de vital importancia para los servicios de seguridad españoles y de los países de los Estados miembros se intercambie con rapidez" (intercambio de información sobre datos personales). El texto, antes de ser aprobado, fue informado por la Agencia Española de Protección de Datos en sentido favorable, entendiendo que con ella se encontraba "un equilibrio" adecuado entre la rapidez y eficacia de la cooperación policial y aduanera, y entre los principios y normas acordados en materia de protección de datos, libertades fundamentales, derechos humanos y libertades individuales, respetando los contenidos jurisprudenciales de las sentencias que en estas materias se adopten por los Tribunales nacionales o internacionales*".*

Según su artículo 1, tiene por objeto[425] "establecer las normas en virtud de las cuales un servicio de seguridad español competente podrá intercambiar con los servicios de seguridad competentes de los Estados miembros de la Unión Europea la información e inteligencia disponibles para llevar a cabo":

[424] B.O.E. número 182, de 28 de julio de 2010. Sec. I. pp. 65770 – 65771.

[425] Artículo 1.

"2. La presente Ley se entenderá sin perjuicio de los Acuerdos Bilaterales o Multilaterales entre el Reino de España y los Estados miembros y terceros países y de los instrumentos de la Unión Europea sobre asistencia jurídica mutua y reconocimiento mutuo de las resoluciones en materia penal, incluida cualquier condición establecida por terceros países relativa al uso de la información una vez facilitada.

3. Esta Ley no será de aplicación al intercambio de información e inteligencia que lleve a cabo el Centro Nacional de Inteligencia en el ámbito de los Acuerdos Internacionales ratificados por el Reino de España en materia de protección mutua de la información clasificada y en el ámbito de las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos Internacionales para el mejor cumplimiento de sus objetivos".

a) Operaciones de inteligencia criminal consistentes en la recogida, tratamiento y análisis de información por los servicios de seguridad competentes sobre delitos o actividades delictivas con carácter previo a la investigación criminal para establecer si se han cometido actos delictivos concretos o se pueden cometer en el futuro.

b) Investigaciones criminales por los servicios de seguridad o las autoridades judiciales competentes encaminadas a adoptar las medidas necesarias para el establecimiento y descubrimiento de los hechos, los sospechosos y las circunstancias en relación con uno o varios actos delictivos concretos comprobados.

Define asimismo la "información e inteligencia", como "todo tipo de información o datos en poder de los servicios de seguridad y, todo tipo de información o datos en poder de autoridades públicas o entes privados, de la que puedan disponer los servicios de seguridad sin tener que utilizar medidas coercitivas definidas de acuerdo con la legislación española. Y los "servicios de seguridad competentes", como las autoridades policiales y aduaneras, que estén autorizadas por el ordenamiento jurídico español para descubrir, prevenir e investigar delitos y actividades delictivas".

Respecto a la protección de datos, contiene un precepto específico, que exige que los "canales de comunicación" y el "procedimiento de intercambio de información e inteligencia", se establezcan "de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en particular con lo dispuesto en su artículo 37" sobre las funciones propias de la Agencia Española de Protección de Datos, autorizando la cesión de datos de carácter personal a los servicios de seguridad competentes de los Estados miembros, a los efectos y fines propios de la Ley.

Para aportar mayor garantía a este tipo de tratamientos por las autoridades policiales, en el contexto europeo, añade finalmente que "los datos personales, que sean objeto de tratamiento en el contexto de la aplicación de esta Ley, están protegidos de conformidad con el Convenio del

Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y, para los Estados miembros que lo hayan ratificado, su Protocolo Adicional, de 8 de noviembre de 2001, relativo a las autoridades de control y los tránsitos transfronterizos de datos. Asimismo, deberán tenerse en cuenta los principios de la Recomendación R (87) 15 del Consejo de Europa, dirigida a regular la utilización de datos de carácter personal en el sector de la policía, cuando los servicios de seguridad manejen datos personales obtenidos en virtud de la presente Ley".

2.2.- Ficheros Policiales.

Todos los ficheros de datos personales que utilizan Policía y Guardia Civil, se encuentran registrados en la Agencia Española de Protección de Datos, bajo la responsabilidad del Ministerio del Interior. El Registro General de Protección de Datos ofrece el listado completo de los ficheros, y su examen resulta muy gráfico a los fines de comprender qué tipo de datos personales pueden ser recabados y tratados por las Fuerzas de Seguridad del Estado.

El acceso a este Catálogo es una posibilidad que deriva del artículo 14 de la LOPD, que permite a cualquier persona conocer de forma pública y gratuita, la existencia de los tratamientos de datos, de sus finalidades y de la identidad del responsable del fichero. Cada fichero inscrito, constata la identidad del responsable del fichero; el servicio o unidad ante el que pueden ejercitarse los derechos de oposición, acceso, rectificación y cancelación; la identificación, finalidad y usos previstos del fichero; el origen de los datos; el colectivo de personas del que se obtienen los datos; el tipo de datos tratados; la estructura y organización del fichero y, en su caso, los destinatarios de cesiones y/o transferencias internacionales de datos. Además, en el caso de los ficheros de titularidad pública, como son los de

las Fuerzas de Seguridad del Estado, es necesario incluir la disposición general de creación, modificación o supresión del fichero.

El Catálogo divide los ficheros del Ministerio del Interior en ficheros de la Policía, ficheros de la Guardia Civil y, ficheros de la Secretaría de Estado de Seguridad[426].

En primer lugar, el análisis del Catálogo de ficheros de la Policía Nacional, nos muestra en primer lugar, que bajo la responsabilidad de la Comisaría General de Extranjería y Documentación, hay cinco ficheros, dedicados a la Gestión del DNI, a la gestión de pasaportes y títulos de personas indocumentadas, a la gestión de informes y resoluciones en materia de extranjería, y a la gestión de antecedentes de personas con "interés policial" (por ejemplo, con órdenes de busca y captura). Además, bajo la responsabilidad de la Comisaría General de Policía Científica, hay seis ficheros dedicados a la identificación de restos humanos de víctimas de hechos catastróficos o criminales y cadáveres de desaparecidos por ADN extraído de los mismos; a la colaboración con la Administración de Justicia en la represión de infracciones penales con identificación genética de vestigios biológicos recogidos en la investigación de presuntos delitos; a la gestión de investigaciones y prestación de servicios de criminalística, identificación analítica e informes periciales, a los órganos judiciales; a la investigación e informes del laboratorio de acústica forense (relacionado con el habla); a la incorporación de reseñas decadactilares de detenidos al sistema de identificación dactilar para su cotejo con huellas anónimas y, a la gestión de archivos y documentos por los servicios centrales de la Comisaría General de Policía.

Bajo la responsabilidad de la Comisaría General de Policía Judicial, hay diez ficheros registrados, dedicados a la gestión de expedientes de investigación de fraudes a la Seguridad Social, a la elaboración de Boletines informativos y estadísticos sobre atracos a entidades bancarias; a la atención a los requerimientos de cooperación internacional necesarios para

[426] Información obtenida del Registro General de Protección de Datos, publicado en la página web de la Agencia Española de Protección de Datos (www.agpd.es), disponible en Noviembre de 2009.

la ejecución de comisiones rogatorias; a la recogida de datos que afecten a infracciones penales dentro del campo de competencia de la Brigada de Patrimonio Histórico; a la atención de requerimientos de cooperación internacional en materia de extradiciones; a la prevención de infracciones penales mediante el análisis de la información generadas por el CNP; al control e inspección de salas de juego; a la gestión de información de órdenes de búsqueda de objetos como el robo de vehículos, armas, documentos de identidad, obras de arte, etc.; al registro de entradas y salidas de la propia Comisaría General de Policía Judicial y, a la ejecución de órdenes de cooperación internacional para el traslados de detenidos.

Bajo la responsabilidad de la Comisaría General de Seguridad Ciudadana, hay cuatro ficheros registrados, dedicados al registro de las actividades del programa de participación ciudadana en el ámbito de la seguridad pública; al registro de las imágenes obtenidas de las grabaciones efectuadas en cumplimiento de la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte; a la gestión de expedientes sancionadores por infracciones de la citada Ley y, al control de actividades de seguridad privada, de empresas y departamentos de seguridad, de vigilantes de seguridad, de vigilantes de explosivos, de escoltas privados, de detectives privados, etc.

Bajo la responsabilidad de la Subdirección General Operativa, hay tres ficheros registrados, dedicados: a la gestión de las actuaciones realizadas para investigar hechos delictivos; a la gestión de comunicaciones de los ciudadanos que informan voluntariamente el lugar de destino de sus vacaciones con el fin de ser informados de incidencias en su domicilio y, a la gestión de trámites de denuncias.

En cuestiones de funcionamiento interno, se encuentra, bajo la responsabilidad de la División de Coordinación Económica y Técnica, un fichero dedicado a gestionar la identificación, autenticación y control de accesos a todas las aplicaciones informáticas de la Dirección General de la Policía. Bajo la responsabilidad de la División de Formación y Perfeccionamiento, hay cuatro ficheros dedicados a: realizar el seguimiento

de alumnos del Centro de Formación; al registro de las actividades deportivas; a la gestión de fondos de la biblioteca (préstamos) y a la gestión de oposiciones y acreditaciones. Bajo la responsabilidad de la División de Personal, hay dos ficheros dedicados a la gestión de reclamaciones económico-administrativas y, a la gestión de recursos humanos (trayectoria profesional, condecoraciones, revistas policiales, etc.).

Por último, bajo la responsabilidad de las Jefaturas de Unidades y Dependencias de la Dirección General de la Policía, se encuentran registrados cuatro ficheros dedicados en general a la gestión de la seguridad de acceso a los centros policiales (formularios del registro de acceso, identificación de personas y vehículos). Bajo la responsabilidad del Jefe Superior de Comisarías Provinciales o Locales, de plantillas que cuenten con un Grupo de atención de menores, se registra un fichero dedicado a la gestión de información correspondiente a menores de edad de interés policial.

En el análisis del Catálogo de ficheros de la Guardia Civil, nos encontramos en primer lugar, que bajo la responsabilidad de la Dirección General de la Guardia Civil, se encuentran registrados ficheros de carácter muy similar a los anteriores, ficheros dedicados a la identificación genética de vestigios biológicos y la identificación genética de muestras de origen conocido; a la identificación genética de personas desaparecidas y cadáveres sin identificar con finalidad científica de interés público y judicial; al control de las materias tipificadas en los reglamentos de armas y explosivos para uso policial; al control y seguimiento de la custodia de las costas y tráfico marítimo; y, a la evaluación de sistemas de reconocimiento de voz; a la identificación de personas por los registros de voz para colaboración con la Administración de Justicia; al mantenimiento de la seguridad ciudadana mediante el control de personas y hechos de interés policial; a incidencias atendidas por equipos de desactivación de explosivos, así como el diseño y efecto de los artefactos empleados en dichas incidencias; a la gestión de habilitaciones concedidas a guardas particulares y, a la gestión de procedimientos sancionadores en materia de seguridad privada.

Bajo la responsabilidad de esta misma unidad, hay otros ficheros dedicados más específicamente a asuntos internos y recursos humanos: a la gestión y control de solicitudes de asistencia letrada del personal de la Guardia Civil por el desempeño de sus funciones; a la tramitación de expedientes disciplinarios; a la gestión del armamento y material de equipamiento policial del personal; a la gestión de tarjetas de identificación del personal adscrito al Cuerpo; a la gestión de uniformes y almacén de vestuario; a la gestión de indemnizaciones por razón del servicio; a la gestión de nóminas, retribuciones y pensiones; a la gestión del IRPF del personal; a la gestión de acuartelamientos (inmuebles y pabellones para uso administrativo); a la gestión del personal del Consejo Asesor de Personal del Cuerpo de la Guardia Civil; al control de actividades deportivas; a la gestión del ingreso de personal y promoción interna (oposiciones y acreditaciones); a la gestión de medallas pensionadas; a la gestión del personal adscrito a la Dirección de la Guardia Civil que no pertenezca al cuerpo; a la evaluación y seguimiento psicológico de los miembros del Cuerpo y de aspirantes; a la gestión de ayudas al estudio concedidas al personal activo; a la gestión de expedientes académicos del personal de la Guardia Civil; a la gestión de permisos de conducir; a la gestión y control de historiales clínicos; a la evaluación de alumnos; al control administrativo y técnico del material y de las horas de vuelo del servicio aéreo; al control de incompatibilidades profesionales; a la identificación y control de accesos a los sistemas informáticos y, a las investigaciones de participación de personal de la Guardia Civil o afecto al mismo, en hechos constitutivos de infracción penal o administrativa, con incidencia en ética personal.

Del análisis del Catálogo de ficheros de la Secretaría de Estado de Seguridad, se desprende en primer lugar que, existen ficheros de organización interna, como los ficheros creados para la gestión de los accesos a la sede del Ministerio del Interior; para la gestión de datos recogidos de los libros de quejas y sugerencias existentes en las Direcciones Generales de Policía y Guardia Civil, y otros órganos de la Administración Pública; y existen ficheros dedicados a recoger información tratada esencialmente para investigaciones policiales, por ejemplo para la identificación genética de personas desaparecidas y cadáveres sin identificar

con la finalidad científica de interés público social y judicial en investigaciones del Ministerio; para la identificación genética de vestigios biológicos y la identificación de muestras de origen conocido en investigaciones realizadas por el Ministerio o, para mejorar la eficacia en la protección de las víctimas de violencia doméstica y de género; facilitar el seguimiento de las circunstancias de riesgo que concurren en ellas; alertar de su evolución permitiendo que se adopten las medidas de protección adecuadas, y prevenir el riesgo de nuevas agresiones.

Bajo la responsabilidad del Gabinete de actuación concertada sobre tráfico de drogas, blanqueo de capitales y delitos conexos, hay un fichero dedicado al registro de la correspondencia y, de entrada y salida de documentación en general y, bajo la responsabilidad del Gabinete de coordinación, hay registrado un fichero para la gestión e identificación de propietarios de vehículos robados, y otro dedicado a recoger la información necesaria para preservar el orden y la seguridad pública y del Estado, así como para la aplicación de las disposiciones del Convenio Schengen sobre la circulación de personas por los territorios de las partes contratantes.

Por último, bajo la responsabilidad del Gabinete de análisis y prospectivas sobre tráfico ilícito de drogas, blanqueo de capitales, y otros delitos conexos, se encuentran los ficheros dedicados a la inscripción de los operadores de las sustancias químicas catalogadas según la Ley 3/1996, de 10 de enero, sobre medidas de control de sustancias químicas catalogadas susceptibles de desvío para la fabricación ilícita de drogas (ya derogada[427]), con actividad en las diferentes Comunidades Autónomas y, un fichero dedicado a la recogida y conservación de información para el seguimiento del cumplimiento de los controles previstos en la referida Ley y, para la transferencia de información a la Agencia Estatal de Administración Tributaria.

Cabe destacar que gran parte de los ficheros observados del Catálogo del Registro Central de Protección de Datos, revisten categorías de

[427] Vigente hasta el 17 de junio de 2009, fecha de entrada en vigor de la Ley 4/2009, de 15 de junio, de control de precursores de drogas. (BOE. núm. 145, de 16 de junio de 2009).

nivel alto de sensibilidad, es decir, que los datos de carácter personal que contienen, han de estar protegidos según lo dispuesto por el artículo 9 de la LOPD, sobre seguridad de los datos y, especialmente, sus responsables deben regirse para ello, por lo dispuesto en los artículos 7 y 8 de la LOPD, sobre datos especialmente protegidos.

2.3.- Seguridad de los Datos.

El tratamiento de información de personas relacionadas con un hecho delictivo, es una parte esencial de las tareas de investigación de las autoridades policiales. El desarrollo tecnológico permite tanto su colección como su almacenamiento en cantidades ingentes, aunque que no siempre es necesario, ni siquiera eficiente. Por ello, para evitar tratamientos altamente invasivos o desproporcionados, para un uso correcto de la tecnología, es importante determinar protocolos de actuación que, en todo Estado de Derecho, deberían ser fijadas en primera instancia por normas de rango constitucional o similar.

En España, señala el artículo 18 de la CE que la ley limitará el uso abusivo de la informática, y su traducción por el Tribunal Constitucional ha derivado en la protección del derecho fundamental a la protección de datos de carácter personal. Su salvaguarda, en la especial naturaleza de los tratamientos realizados por las autoridades policiales, viene recogido en el artículo 22: "Ficheros de las Fuerzas y Cuerpos de Seguridad".

En primer lugar hay que recordar que la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, entiende como tales, a las Fuerzas y Cuerpos de Seguridad del Estado dependientes del Gobierno de la Nación (Cuerpo Nacional de Policía y Guardia Civil), los dependientes de las Comunidades Autónomas (Cataluña, País Vasco y Navarra) y, los dependientes de las Corporaciones Locales. En segundo lugar, que las

Agencias De Protección de Datos de Cataluña y País Vasco, tienen competencias directas sobre los ficheros creados por las Administraciones Públicas, en el caso que nos ocupa, de los especiales ficheros de los Mossos d' Escuadra y Ertainza. El resto de los ficheros, dependen directamente de la Agencia Española de Protección de Datos según lo visto el apartado anterior.

En el año 1987 la Recomendación R (87) 15 del Comité de Ministros del Consejo de Europa a los Estados miembros, vino a regular el uso de datos personales en el ámbito policial[428]. Sus principios clave requerían una debida diligencia en[429] actuaciones tales como:

1.- Control y notificación de ficheros: La gestión de ficheros de datos de carácter personal con finalidades policiales, deben ser registrados por una autoridad de control independiente, que vele por su correcta gestión.

2.- Tratamientos necesarios: la colección y almacenamiento de los datos personales debe ser necesaria para la detección y represión de hechos delictivos que se estén investigando, y debe hacerse exclusivamente para esta finalidad.

3.- Tratamientos de carácter temporal: los datos deben ser almacenados con carácter temporal, por el tiempo estrictamente necesario que sirvan a los fines de la investigación y, en todo caso, deben ser actualizados en la medida que lo requiera la duración de la actividad policial. Los datos deberán eliminarse cuando pierdan su finalidad originaria.

4.- Comunicación o cesión de datos: los datos sólo podrán ser comunicados a terceros en caso de ser estrictamente necesario, que exista un interés legítimo o una habilitación legal que lo permita, salvo

[428] Disponible en Policing OnLine Information System : http://polis.osce.org/library/f/2670/471/CoE-FRA-RPT-2670-EN-Recommendation%20No.%20R(87)%2015.pdf (Noviembre 2009).
[429] ZAMBRANO GÓMEZ, E. "La regulación de los ficheros policiales en España y su tratamiento en la Convención de Prüm: la perspectiva de las autoridades nacionales de protección de datos". *Revista Española de Derecho Constitucional Europeo*, nº 7, Enero – Junio (2007), pp. 167-180. http://www.ugr.es/~redce/

que exista un peligro grave inminente que lo requiera. Además, habrá de tenerse en cuenta que el tratamiento posterior de los datos, deberá estar directamente relacionado, y ser compatible, con aquel para el que fueron recabados los datos.

5.- Custodia diligente: los datos deben ser tratados y custodiados con la debida diligencia y, para ello, deberán implantarse las medidas de seguridad técnicas y lógicas que sea necesario.

Los tratamientos de datos realizados por las autoridades policiales, pueden ser tratamientos de carácter puramente administrativo, o pueden tener finalidades estrictamente policiales. Los primeros, implican la actividades como la expedición de documentos identificativos, controles fronterizos, controles de tráfico, regularizaciones en materia de extranjería, o tratamientos relativos a la propia actividad administrativa o burocrática de las Fuerzas y Cuerpos de Seguridad, como administración pública que son. Y los segundos, son los que están específicamente relacionados con la seguridad del Estado.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, estableció cierta flexibilidad para que los Estados miembros pudieran tomar decisiones de cierta envergadura en la imposición de límites a las obligaciones generales de su texto, cuando tal limitación constituyese una medida necesaria para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales. Es decir, prevé que excepcionalmente los Estados Miembros puedan adoptar nuevas medidas de seguridad, o límites a éstas, en función de la naturaleza de las acciones ante las que se encontrasen las autoridades policiales[430].

[430] Por ejemplo, el artículo 13 de la Directiva 95/46/CE, al prever estas limitaciones, y para el caso concreto del derecho de acceso de los ciudadanos a la información personal que de ellos pueda manejar la Administración Pública, señala en su segundo apartado que: "Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante

La normativa Española, en transposición de aquella, ha establecido con la LOPD el régimen general de protección de datos, pero en materia de seguridad de estado o de orden público, ha dejado al margen los ficheros de carácter público creados para la investigación del terrorismo y de formas graves de la delincuencia organizada.

El propio artículo 3.2 de la Directiva 95/46/CE, excluyó de su aplicación el tratamiento de datos personales "efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal". Pero no quiere esto decir que no vayan a estar sometidos a los principios constitucionales básicos de respeto al derecho fundamental a la protección de los datos personales, e incluso de otros derechos humanos como el derecho al secreto de las comunicaciones o el derecho a la intimidad, puesto que, en todo caso, la Agencia de Protección de Datos ha de estar informada de las circunstancias de creación (características y finalidad) de dichos ficheros y, de las garantías y procedimientos judiciales establecidos para la protección de los derechos fundamentales, pues son del todo aplicables a los tratamientos de datos realizados por las autoridades policiales.

Los ficheros policiales creados para la recogida y tratamiento de datos personales por parte de las Fuerzas y Cuerpos de Seguridad, con exclusivos fines policiales, habrán de seguir un régimen especial dentro del régimen general, por el interés general que están destinados a cubrir.

---

una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas".

Esas previsiones aparecen recogidas en los artículos 22 a 24 de la LOPD, y de ellas se desprenden las siguientes directrices que guiarán su tratamiento:

a) "Van a estar limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

b) Deben ser almacenados en ficheros específicos establecidos al efecto.

c) Deben clasificarse por categorías, en función de su grado de fiabilidad".

d) Los tratamientos de datos personales que revelen la ideología, afiliación sindical, religión y creencias, origen racial, la salud y la vida sexual, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

e) Los datos personales se cancelarán cuando no sean necesarios para las investigaciones policiales que motivaron su almacenamiento.

Además se prevén ciertas excepciones a las posibilidades de control que sobre su propia información tienen los afectados o titulares de los datos. Se trata de excepciones a los derechos de acceso, rectificación y cancelación, por cuanto tales derechos podrán ser denegados "en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las

necesidades de las investigaciones que se estén realizando"[431]. Pero a pesar de ello, no se deja al ciudadano desprovisto de garantías, pues siempre podrá poner estas circunstancias en conocimiento del Director de la Agencia Española de Protección de Datos o del organismo competente de cada Comunidad Autónoma, cuyos responsables (en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas) deberán asegurarse de la procedencia o improcedencia de la denegación[432].

Otras excepción respecto del régimen general, se prevé en la normativa para el hecho de que la recogida de datos para fines policiales pueda hacerse sin consentimiento del interesado (en todo caso, sólo en aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales). Se podrá prescindir por ejemplo de la información que en circunstancias normales habría de proporcionarse al afectado, como la existencia de un fichero, la posibilidad de ejercitar aquellos derechos de acceso, rectificación y cancelación, la identidad y dirección del responsable del tratamiento, las consecuencias de la negativa a suministrar datos, o el carácter obligatorio o facultativo de los datos, cuando pueda afectar a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales[433].

En el aspecto técnico de la protección, las medidas de seguridad que deberán implementarse para la diligente protección de los ficheros que almacenan datos de carácter personal, que en definitiva van a ser objeto de tratamiento[434] por las autoridades policiales, han de ser de nivel medio en general, sobre todo para los ficheros relativos a la comisión de infracciones penales. Sin embargo, cuando contengan datos recabados sin

[431] Artículo 23.1 de la LOPD.

[432] Artículo 12.2.c) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos. "Corresponde al Director de la Agencia Española de Protección de Datos dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia y, en especial: Resolver motivadamente, previo informe del responsable del fichero, sobre la procedencia o improcedencia de la denegación, total o parcial, del acceso a los ficheros policiales o tributarios automatizados".

[433] Artículo 24 de la LOPD y, en relación directa, los ficheros creados al amparo de la Ley 12/2003, de 21 de mayo, de prevención y bloqueo de la financiación del terrorismo.

[434] Artículo 81 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

consentimiento de las personas afectadas, para esos fines policiales, o bien se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, deberán estar protegidos por un sistema de seguridad de nivel alto. A todo ello, además, se deberá añadir la más evidente de las medidas de seguridad en cuanto al cumplimiento de la lógica confidencialidad de todo tratamientos: el deber de secreto previsto por el artículo 10 de la LOPD y, específicamente, por el artículo 5.5 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad: "Secreto profesional- deberán guardar riguroso secreto respecto a todas las informaciones que conozcan por razón o con ocasión del desempeño de sus funciones. No estarán obligados a revelar las fuentes de información salvo que el ejercicio de sus funciones o las disposiciones de la Ley les impongan actuar de otra manera"[435].

Finalmente, respecto de la posibilidad que tienen las autoridades policiales de ceder o comunicar los datos de carácter personal que se contienen en sus ficheros, siempre por razones de la necesaria cooperación con otros organismos, y en aras de eficiencia en la investigación, hay que recordar que estas actuaciones deben estar regidas también por protocolos de seguridad y garantías de confidencialidad que impidan el acceso a los mismo por terceros no autorizados, impidiendo toda manipulación ilícita de estas informaciones. Si bien es cierto que la protección de los datos personales es importante, no lo es menos que "la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana. Bienes igualmente reconocidos en los arts. 10.1 y 104.1 de la CE"[436].

---

[435] Ver además los artículos 7.17 y 8.11 de la Ley Orgánica 12/2007, de 22 de octubre, del régimen disciplinario de la Guardia Civil, sobre la violación del secreto profesional, especialmente grave "cuando afecte a la defensa nacional o a la seguridad ciudadana, perjudique el desarrollo de la labor policial o cause daños a personas físicas o jurídicas, públicas o privadas". Similar a lo previsto por el Real Decreto 884/1989, de 14 de julio, por el que se aprueba el Reglamento de Régimen Disciplinario del Cuerpo Nacional de Policía, en su artículo 6.7: "La violación del secreto profesional y la falta del debido sigilo respecto a los asuntos que conozcan por razón de su cargo, que perjudique el desarrollo de la labor policial o a cualquier persona".

[436] Sentencia 292/2000, de de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (F.Jº. 9º): "En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el artículo 105 b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" (en relación con el

La comunicación de datos personales entre las Fuerzas y Cuerpos de Seguridad, para la colaboración de las distintas unidades y organismos que las componen (tanto nacionales como internacionales), debe ser una medida "necesaria y proporcionada" en un Estado de Derecho, porque no se trata de procesar grandes volúmenes de información, sino de hacerlo en tiempo real, de forma ágil y eficiente[437]. Así lo recogía ya "el Convenio Europeo de 1981, en su artículo 9. Al igual que el Tribunal Europeo de Derechos Humanos, quien refiriéndose a la garantía de la intimidad individual y familiar del artículo 8 CEDH, aplicable también al tráfico de datos de carácter personal, reconociendo que pudiera tener límites como la seguridad del Estado (STEDH caso Leander, de 26 de marzo de 1987, §§ 47 y sigs.), o la persecución de infracciones penales (mutatis mutandis, SSTEDH, casos Z, de 25 de febrero de 1997, y Funke, de 25 de febrero de 1993), ha exigido que tales limitaciones estén previstas legalmente y sean las indispensables en una sociedad democrática, lo que implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito (Sentencias del Tribunal Europeo de Derechos Humanos, caso X e Y, de 26 de marzo de 1985; caso Leander, de 26 de marzo de 1987; caso Gaskin, de 7 de julio de 1989; mutatis mutandis, caso Funke, de 25 de febrero de 1993; caso Z, de 25 de febrero de 1997)"[438].

El Tribunal Constitucional español ha establecido estos límites basándose en el principio de proporcionalidad pero en sus dos vertientes, de idoneidad e intervención mínima[439]. Su doctrina entiende, en el caso concreto de la protección de datos personales (STC 292/2000, de 30 de

---

artículo 8.1 y 18.1 y 4 CE), y en numerosas ocasiones este Tribunal ha dicho que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana. Bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE (por citar las más recientes, SSTC 166/1999, de 27 de septiembre, F.Jº. 2º, y 127/2000, de 16 de mayo, F.Jº. 3º.a; ATC 155/1999, de 14 de junio)".

[437] El Grupo de Análisis y Tratamiento de la Información (G.A.T.I.), perteneciente a la Comisaría General de Policía Judicial, proporciona los medios necesarios para un tratamiento eficiente de la información en manos de la Policía Nacional, a través de sus sistemas informáticos, a los fines de la prevención y represión de infracciones penales y el mantenimiento del orden público.

[438] Op. Cit. STC 292/2000 (F.Jº. 9º) ...

[439] MARTÍNEZ MARTÍNEZ, R. "Ficheros Policiales y Constitución". *Revista Datos Personales de la APDCM* Nº 16, Julio 2005. www.datospersonales.org

Noviembre, F.Jº. 11º), que justamente, "si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos.

Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional".

Proyectos como el llamado "Proyecto SUBA" (Sistema Unificado de consultas de las Bases de Datos), puesto en marcha por el Ministerio del Interior en el año 2004, pretendían coordinar la actividad de los cuerpos de policía, permitiéndoles en aquel caso acceder a seis bases de datos personales que se coordinarían para permitir un acceso común y compartido, aumentando la eficacia de las actuaciones en prevención de las amenazas terroristas. Las bases de datos en juego serían aquellas que

contienen información sobre el Documento Nacional de Identidad y tarjetas de residencia (identificación de extranjeros en España), sobre armas y explosivos, sobre alquiler de vehículos y viajeros, sobre reconocimiento de voces y, sobre huellas dactilares y datos genéticos.

Este proyecto sumaba esfuerzos a otras iniciativas de coordinación gestionadas por la Secretaría de Estado de Seguridad del Ministerio del Interior, como las denominadas SIRENE (espacio Schengen), PERPOL (coordinación judicial) o ADEXTRA (extranjería). Y fuera quedaban otras bases de información como la denominada GATI.

En ese mismo año, en todo el ámbito europeo se conocieron gran número de propuestas que pretendían incrementar y optimizar el intercambio de datos personales entre las fuerzas y cuerpos de seguridad de los Estados Miembros, en el marco de la lucha contra el terrorismo y el crimen organizado. El atentado perpetrado en Madrid el 11 de marzo de 2004 supuso un importante hito en cuanto el sentido en que se sucedieron los debates sobre la seguridad en Europa, que ya estaban siendo presididos por las actuaciones que desde los atentados el 11 de septiembre de 2001 se venían desarrollando en Estados Unidos.

Por ejemplo, en materia de coordinación policial, cabe destacar la "Comunicación de la Comisión sobre medidas para combatir el terrorismo y otras formas graves de delincuencia, en particular mediante la mejora de los intercambios de información, de 29 de marzo de 2004, o el Proyecto de decisión Proyecto de Decisión Marco sobre la simplificación del intercambio de información e inteligencia entre las fuerzas y cuerpos de seguridad de los Estados miembros de la UE, en particular en relación con formas graves de delincuencia incluyendo actos de terrorismo", de 4 de junio de 2004. Un tercer documento planteado en este sentido fue la Comunicación de la Comisión "Hacia una mejora del acceso a la información por parte de las fuerzas y cuerpos de seguridad", de 16 de junio de 2004.

De todas estas iniciativas, pueden extraerse tres conclusiones para el desarrollo posterior de actuaciones policiales antiterroristas en el ámbito

de la Unión Europea: una cooperación más estrecha entre las policías de los Estados miembros, el tratamiento e intercambio de más datos personales y, la conexión efectiva entre la lucha contra el terrorismo y la lucha contra el crimen organizado. Así lo reconocía por ejemplo la Comunicación de la Comisión al Consejo y al Parlamento Europeo[440], en Diciembre de 2005, sobre los tres principales sistemas de información de que dispone en la actualidad la Unión Europea: SIS II, VIS y EURODAC, cuando decía que "la seguridad de los ciudadanos europeos constituye una preocupación capital, sobre todo tras los recientes atentados terroristas. Es imprescindible prevenir toda radicalización y proteger nuestras infraestructuras esenciales. Conviene también perfeccionar la colaboración con terceros países en todos los ámbitos relacionados con la justicia y los asuntos de interior. Esta cooperación debería aprovechar los mecanismos existentes para luchar contra el terrorismo, la trata de seres humanos y el tráfico de estupefacientes. La Presidencia y el Coordinador en materia de lucha contra el terrorismo han presentado una propuesta relativa a una estrategia europea contra el terrorismo, que será examinada por el Consejo Europeo de diciembre de 2005. En el ámbito de la lucha antiterrorista, la Comisión cumple las obligaciones que le corresponden conforme al plan de acción adoptado tras los atentados de Madrid y el programa de La Haya. Se tiene en cuenta el nuevo calendario establecido tras los atentados de Londres. El año próximo será crucial para la aplicación de las políticas y propuestas legislativas presentadas en 2005 por la Comisión, por ejemplo en lo tocante al intercambio de información (principio de disponibilidad), incluidos la protección de datos y el acceso al sistema de información sobre los visados, la radicalización y el reclutamiento de terroristas, la protección de las infraestructuras básicas y la financiación del terrorismo y los explosivos"[441].

[440] Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 24 de noviembre de 2005, sobre una mayor eficacia, interoperabilidad y sinergia entre las bases de datos europeas en el ámbito de la Justicia y los Asuntos de Interior [COM (2005) 597 final - no publicada en el Diario Oficial]. Los principales objetivos de la Comunicación se pueden resumir en: "mejorar la interoperabilidad técnica y las sinergias entre los sistemas existentes de información (SIS II, VIS, EURODAC) en los ámbitos de Justicia y Asuntos de Interior (JAI); destacar de qué forma estos sistemas podrían constituir un apoyo para las políticas relacionadas con la libre circulación, la lucha contra el terrorismo y la delincuencia organizada, respetando al mismo tiempo la protección de los derechos fundamentales; iniciar un debate en profundidad sobre la forma y la arquitectura a largo plazo de los sistemas de información".

[441] Informe provisional sobre el seguimiento de la reunión informal de Jefes de Estado y de Gobierno celebrada en Hampton Court, el 27 de octubre de 2005, sobre la respuesta de Europa ante la globalización.

En esta misma línea de preocupación por coordinar la lucha antiterrorista, y por la realización de un espacio eficiente de justicia, libertad y seguridad, se han sumado otras propuestas como las recogidas por la Decisión 2007/125/JAI del Consejo, de 12 de febrero de 2007, por la que se establece para el período 2007-2013 el programa específico Prevención y lucha contra la delincuencia, integrado en el programa general Seguridad y defensa de las libertades, que prevé en particular el "intensificar la coordinación y la cooperación entre los servicios policiales, las otras autoridades nacionales y los órganos de la UE, favorecer las buenas prácticas en materia de protección de las víctimas y los testigos y, fomentar los métodos necesarios para una estrategia de prevención y lucha contra la delincuencia y para el mantenimiento de la seguridad, tales como las actividades de la red europea de prevención de la delincuencia y las asociaciones entre las instancias públicas y privadas", o las Decisiones 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza; la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

2.4.- Criterios de la AEPD.

"La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones"[442], y que en el cumplimiento de sus tareas se rige

[442] Artículo 35.1 de la LOPD.

por lo dispuesto por el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos[443].

Las funciones de la Agencia Española de Protección de Datos[444] se centran en velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación (en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos), y para ello, puede emitir autorizaciones; dictar las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley; atender peticiones y reclamaciones de los titulares de datos de carácter personal; proporcionarles información sobre sus derechos en esta materia; recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones; requerir a los responsables y los encargados de los tratamientos la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la Ley; ordenar la cesación de tratamientos y la cancelación de ficheros; ejercer la potestad sancionadora; informar los proyectos de disposiciones generales que desarrollen la LOPD; velar por la publicidad de la existencia de ficheros de datos con carácter personal; dictar las instrucciones precisas sobre las condiciones de seguridad de los ficheros; redactar una memoria anual y remitirla al Ministerio de Justicia, y desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

En relación con los individuos afectados por un tratamiento de datos de carácter personal, ante la posibilidad de que ese tratamiento pueda ser sometido a inspección por parte de la AEPD, se presenta la tarea esencial de informar en primera instancia sobre las condiciones de aplicación de la LOPD[445]. Para ello, dispone especialmente de la capacidad de promover campañas de difusión, de colaborar con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas, dictando

[443] El Estatuto de la AEPD ha sido modificado por el Real Decreto 1665/2008, de 17 de octubre, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo; y matizado por la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social y la Ley 12/1995, de 11 de mayo, de Incompatibilidades de los Miembros del Gobierno de la Nación y de los Altos Cargos de la Administración General del Estado.
[444] Artículo 37 de la LOPD.
[445] Artículos 4, 5 y 8 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica y, de dictar resoluciones precisas en los casos planteados por los destinatarios de la LOPD. La experiencia de todo ello, quedará finalmente reflejada en una Memoria anual que se elaborará con directrices concretas sobre la aplicación de la Ley Orgánica 5/1992, y las demás disposiciones legales y reglamentarias sobre protección de datos. Contendrá además una relación de los códigos tipo, un análisis de las tendencias legislativas, jurisprudenciales y doctrinales de los distintos países en materia de protección de datos y, un análisis y una valoración de los problemas de la protección de datos a escala nacional.

Si bien en materia de protección de datos y ficheros policiales, la práctica ha dado lugar a pocas resoluciones de la AEPD[446], las cuestiones más confusas sobre las que el ente público se ha pronunciado casi siempre han sido en relación con solicitudes de acceso, rectificación y cancelación o bloqueo de antecedentes penales, así como el derecho a ser informado en lo relativo a la recopilación o tratamiento de datos personales por las autoridades policiales o judiciales correspondientes.

Conviene analizar algunas de estas resoluciones para conocer cual es el criterio habitual de la AEPD.

Respecto de las competencias de las autoridades policiales para recabar datos de carácter personal, sin el consentimiento del afectado, la AEPD considera que debe serle de aplicación el artículo 6 de la LOPD, en relación directa con el artículo 6. 11. 1. h) de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, que señala expresamente que "las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones: Captar, recibir y analizar cuantos datos tengan interés para el orden y la Seguridad Pública, y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia*".* Es decir, que para la realización de estas funciones, la

[446] Según la Memoria del año 2008 de la AEPD, entre el año 2007 y el 2008, tan sólo se han planteado cuatro consultas en materia de ficheros policiales.

Administración Pública no necesita recabar el consentimiento del afectado, por cuanto se trata del ejercicio de funciones propias de la Administración Pública en el ámbito de sus competencias[447].

Otra cuestión que ha sido analizada es la exigencia legal de que los datos tratados por las autoridades cumplan con el requisito de la calidad[448], especialmente, el hecho de que estén actualizados al momento de ser considerados cualquiera que sea su finalidad. En este sentido, se planteó una cuestión sobre la concesión de una licencia de armas y el almacenamiento de antecedentes penales en el fichero denominado INTPOL, perteneciente a la Dirección General de la Guardia Civil, cuya finalidad declarada era el "mantenimiento de la seguridad ciudadana mediante el control de personas y hechos de interés policial" en actuaciones previstas en el marco de la seguridad e investigación policial y, en "diligencias instruidas con ocasión de actuaciones policiales, reseña de detenidos, denuncias recibidas y órdenes judiciales de requisitoria". Reclamaba el titular de los datos personales que sus datos fuesen actualizados en dicho fichero, sin embargo, entendió la AEPD[449] que las autoridades policiales sometidas a inspección tenían competencias legalmente reconocidas para realizar cuantas investigaciones fueran necesarias sobre los antecedentes del interesado, y ello en relación directa con la aplicación de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, y el RD 137/1993, de 29 de enero, por el que se aprueba el Reglamento de Armas.

A parte de estas cuestiones, la cancelación de los datos personales ha sido con diferencia la cuestión más controvertida en consultas sometidas a la AEPD sobre ficheros policiales. Las consecuencias negativas que supone

[447] Resolución de Archivo de Actuaciones, Expediente nº E/00144/2004, de fecha 20 de mayo de 2005.

[448] Calidad de los datos: El Artículo 4 de la LOPD recoge los requisitos esenciales de dicha calidad y, se resumen en que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido; no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos (no se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos); serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado; (si los datos almacenados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados); serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados, es decir, no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

[449] Resolución de Archivo de Actuaciones, Expediente nº E/00464/2004, de fecha 28 de abril de 2004.

para los afectados el verse calificado por las Administraciones Públicas como "delincuente" y, sobre todo, el hecho de que no siempre se conozca el alcance de dichos registros, o hasta qué punto pueden afectar negativamente a su vida y decisiones futuras, ha supuesto que deban ser las resoluciones de un ente público las que finalmente orienten a los ciudadanos sobre sus derechos en esta materia.

De las resoluciones habidas hasta el momento, el principal problema que se observa es la consideración de los antecedentes policiales como necesarios para las investigaciones que ocasionaron su recogida. Analizando el contenido de algunas de estas resoluciones[450], es necesario en primer lugar matizar la distinción entre antecedentes penales y policiales. Los primeros, dimanan de una sentencia judicial, y han de regirse por lo dispuesto en los artículos 136 y 137 del Código Penal, en base a que "los condenados que hayan extinguido su responsabilidad penal tienen derecho a obtener del Ministerio de Justicia, de oficio o a instancia de parte, la cancelación de sus antecedentes penales, previo informe del juez o tribunal sentenciador".

Los antecedentes policiales, los ficheros de las fuerzas y cuerpos de seguridad que los contienen se rigen por lo dispuesto en la LOPD y, en su defecto, deberán ajustarse a las leyes específicas que los regulan.

El artículo 4.1 de la LOPD establece con carácter general el principio de calidad de los datos, que sólo podrán ser recabados sometidos a tratamiento, cuando sean "adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". El artículo 22.2 de la LOPD habilita la recogida de datos de carácter personal y su tratamiento, sin consentimiento del afectado, en materia de tratamientos policiales, siempre y cuando sea para supuestos (y categorías de datos) "necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales", de

[450] Resolución nº R/00759/2005, de fecha 28 de octubre de 2005; Resolución nº R/00611/2006, de fecha 8 de septiembre de 2006; Resolución nº R/00897/2006, de fecha 30 de noviembre de 2006; Resolución de Archivo de Actuaciones, Expediente nº E/00222/2007, de fecha 27 de febrero de 2009; Resolución nº R/00860/2008, de fecha 24 de julio de 2008; Resolución nº R/00106/2009, de fecha 30 de enero de 2009.

modo que todo ello queda condicionado a que fueran necesarios para las averiguaciones que lo motivaron y a la necesidad de mantenerlos hasta la conclusión de una investigación o procedimiento concreto[451]. Estos datos deben ser almacenados en ficheros específicos, clasificados por categorías en función de su grado de fiabilidad, y deben ser cancelados cuando la finalidad de prevención o represión de infracciones penales prevista por Ley deje de existir (por ejemplo, en el caso de sentencias absolutorias firmes o sobreseimientos provisionales, en los que no haya sido posible acreditarse la autoría de los hechos que motivaron la formación de la causa, y por tanto, nunca hubo registro de antecedentes penales).

Los límites o excepciones a esta cancelación, son la exigencia de un plazo de 10 días para que la entidad requerida para la cancelación de los datos emita una respuesta por (artículo 16 de la LOPD) y, el denominado "bloqueo" de los datos, que implicará la reserva de los mismos sin llegar a su destrucción.

Los responsables de los ficheros policiales podrán denegar la cancelación, el acceso o la rectificación de datos personales tomando en consideración los peligros que de ello pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando (artículo 23 de la LOPD) y, en este sentido, procederán al bloqueo de los datos, "conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas" (artículo 16.3 de la LOPD)[452]. El artículo 5 del Reglamento de

[451] Artículo 22.3 de la LOPD: "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas estén limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad". En relación con el artículo 4.5 de la LOPD: "Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento integro de determinados datos".

[452] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Artículo 8. 6

desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, establece idéntica finalidad[453].

Teniendo en cuenta la especial finalidad de los datos de carácter personal almacenados en los ficheros de las fuerzas y cuerpos de seguridad, es comprensible que en la mayoría de las ocasiones se proceda a ese bloqueo sin más y, si se tiene en cuenta el criterio "salvaguarda de amenazas terroristas", como motor de transformaciones severas en las doctrinas y normativa de protección de datos a nivel mundial, es comprensible que se pretenda la conservación de datos personales de cualquier carácter el mayor tiempo posible. Véase por ejemplo, la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, pues aunque se basa en la Directiva 2002/58/CE[454], cuando establece que "tales restricciones deben constituir medidas necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público, como proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, detección y enjuiciamiento de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas", lo cierto es que esta normativa de conservación de datos personales fue prevista para la prevención, investigación, detección y enjuiciamiento de delitos, es decir, con finalidades policiales.

Principios relativos a la calidad de los datos: "Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado. Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento". Artículo 33. 1. "Denegación de los derechos de rectificación y cancelación: La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos".

[453] (…) "con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades".

[454] Artículo 15, apartado 1, de la Directiva 2002/58/CE fija las condiciones en que los Estados miembros pueden limitar el alcance de los derechos y obligaciones que se establecen en el artículo 5, el artículo 6, el artículo 8, apartados 1 a 4, y el artículo 9 de dicha Directiva.

IV.- FICHEROS ESPECÍFICOS DE CONTROL ESTATAL.

1.- Control de las comunicaciones electrónicas.

En la complicada tarea de delimitar el uso de la tecnología sobre los ciudadanos, se encuentra la importante cuestión de las comunicaciones electrónicas, pues son por si mismas tanto herramienta de control, como fuente inagotable de información, y pueden resultar tan útiles como lesivas para quienes las utilizan.

El progresivo incremento de la capacidad de actuación de las tecnologías existentes hoy en día, y su puesta en el mercado de forma asequible para los consumidores individuales, ha llevado a que las comunicaciones electrónicas sean una pieza imprescindible de nuestra forma de entablar relaciones sociales y de convivencia[455]. Constituyen la

[455] La aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación mediante una expansión de los contenidos transmitidos, que abarcan no solo la voz, sino también datos en soportes y formatos diversos.

infraestructura sobre la que se construye la "Sociedad de la Información" y del conocimiento, pero además, son la infraestructura perfecta para amparar nuevas formas de criminalidad que pueden afectar gravemente a la seguridad de quienes se sirven de ellas, simplemente con la mera manipulación de los datos que se transmiten a través dichas comunicaciones.

La información puede ser de todo tipo y puede adoptar diferentes formas, ya sean sonidos, datos o imágenes, pero lo que es claro es que su protección, ha de serlo en función del significado de su contenido.

Teniendo en cuenta que son las personas físicas las que utilizan como usuarios finales las comunicaciones electrónicas, y que son ellas las que finalmente quedarían afectadas si se diera una utilización maliciosa de los detalles de dichas comunicaciones, los Estados deben buscar continuamente fórmulas que les permitan protegerlas. No se puede olvidar que dicha protección se puede lograr tanto con la tecnología como con la regulación legal de su uso. Para ello, es conveniente observar los efectos de la implantación práctica de todo avance tecnológico, para obtener así respuestas eficientes a las nuevas necesidades que van surgiendo para sus ciudadanos y la protección de sus derechos. Aunque habitualmente sucede que antes de que se termine de conocer una tecnología de transmisión de información, ya han aparecido otras nuevas que la sustituyen, con diferentes y novedosos efectos. La rapidez con que se están produciendo estos cambios, unida a la impaciencia por dar respuestas a sus efectos, están provocando que los Estados valoren incorrectamente la utilidad que aportan o cómo influyen en las relaciones humanas, especialmente, en nuestra esfera privada.

En el caso de las comunicaciones electrónicas, las tareas de concretar su uso y de supervisarlo, se está convirtiendo para los gobiernos

---

A su vez, esta extraordinaria expansión en cantidad y calidad ha venido acompañada de un descenso en los costes, haciendo que este tipo de comunicaciones se encuentren al alcance de cualquier persona y en cualquier rincón del mundo. La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines inadecuados, cuando no delictivos. Preámbulo de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

en un objetivo complejo que no siempre muestra claramente los límites aplicables.

El derecho a utilizar la tecnología, la protección efectiva de sus usuarios y, la vigilancia indiscriminada de sus movimientos, necesita un marco claro de actuación con equilibrio entre la protección de la seguridad pública y el respeto a los derechos individuales, tales como los relativos a la intimidad, la protección de datos y, el secreto de las comunicaciones. Cualquier intervención en aspectos privados de la comunidad ha de estar plenamente justificada en su adopción y supervisada en su ejecución.

En todo Estado de Derecho, el poder judicial tiene en principio las competencias necesarias para velar por el equilibrio de intereses en juego en la comunidad, y también cuando el uso de la tecnología puede afectar derechos fundamentales como el derecho al secreto de las comunicaciones, para lo cual deberá considerar en todo caso los límites de lo excepcional en la situación que se trate de "vigilar". La normativa española vigente prevé garantías de naturaleza constitucional para que la observación de las comunicaciones de los ciudadanos, o de las relaciones de la comunidad, se realice siempre manteniendo el equilibrio necesario. El artículo 18 de la CE[456] señala expresamente que "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial". La Constitución, consciente de la evolución continua de la tecnología, posibilita incluso la adaptación de sus presupuestos señalando expresamente que la ley limitará el uso de la informática para garantizar el pleno ejercicio de los derechos de los ciudadanos.

A lo largo de la historia, y a nivel internacional, han sido muchos los sistemas y programas de seguridad estatal que, contando con respaldo gubernativo, han sido implantados para controlar las relaciones de la

[456] Artículo 18 CE: "1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

comunidad con la mayor independencia y amplitud posible. En los últimos tiempos, y lógicamente cada vez con más éxito, se ido poniendo en marcha distintos programas de interceptación de comunicaciones, como el conocido ECHELON, el sistema de vigilancia más importante del mundo, diseñado por la Agencia de Seguridad Nacional de Estados Unidos en los años 70, y que en teoría se utiliza para escuchar comunicaciones realizadas por teléfono, fax o correo electrónico, desde países considerados enemigos. En Europa, ya en 1995, fue creado a su imagen y semejanza, el programa llamado ENFOPOL. Ambos sistemas fueron implantados bajo el más riguroso secretismo, debido a que en la mayoría de las ocasiones sus actividades pertenecían al ámbito de las denominadas "materias reservadas", que son parte de la función directiva gubernamental para la defensa nacional, pero el problema es que no siempre se ha limitado su uso a estas tareas y, se han podido invadido esferas propias de la dignidad del ser humano con total impunidad.

1.1.- Secreto de las comunicaciones:

1.1.a.- El concepto.

El derecho al secreto de las comunicaciones está reconocido universalmente como un derecho fundamental de las personas, y tiene protección reglada prácticamente desde la Revolución francesa. Es más, hoy aún se reconocen como vigentes normas históricas del nivel de la Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948, que en su artículo 12 expone: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni ataques a su honra o reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias o ataques".

En similares términos se expresa también el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos, aprobado con fecha 16 de diciembre de 1966: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia , ni de ataques ilegales a su honra y reputación". Por su parte, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH) de 1950, en su artículo 8 reconoce textualmente el "Derecho al respeto a la vida privada y familiar: 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia éste prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

En el ámbito europeo, la Proclamación de la Carta de Derechos Fundamentales de la Unión Europea del año 2000, contiene un artículo 7, previo al reconocimiento del derecho a la protección de datos, que estableció el "Respeto de la vida privada y familiar: Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones". Y siguen a esta afirmación, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en busca de la armonización de las garantías frente a las intervenciones en cualquier medio de comunicación, aunque dejó fuera de su ámbito de aplicación las medidas que puedan adoptar los Estados "para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, investigación, detección o persecución de delitos" (artículo 15.1) y, la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de

comunicaciones, por la que se modifica la Directiva 2002/58/CE y, la Directiva 97/67/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa a las normas comunes para el desarrollo del mercado interior de los servicios postales de la Comunidad y la mejora de la calidad del servicio[457]. Otras Directivas relacionadas con esta materia son Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso); la Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización); la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco); la Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal), y la Directiva 2002/77/CE, de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas.

Pero la norma más importante en esta materia es sin duda la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas ("Directiva sobre la privacidad y las comunicaciones electrónicas")[458], porque su artículo 5

[457] Artículos 1 a 11 y, artículos 22 a 28.

[458] Considerandos: (2) "La presente Directiva pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea. Señaladamente, la presente Directiva pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de dicha Carta. (3) La confidencialidad de las comunicaciones está garantizada de conformidad con los instrumentos internacionales relativos a los derechos humanos, especialmente el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y las constituciones de los Estados miembros. (5) Actualmente se están introduciendo en las redes públicas de comunicación de la Comunidad nuevas tecnologías digitales avanzadas que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios. El desarrollo de la sociedad de la información se caracteriza por la introducción de nuevos servicios de comunicaciones electrónicas. El acceso a las redes móviles digitales está ya disponible y resulta asequible para un público muy amplio. Estas redes digitales poseen gran capacidad y muchas posibilidades en materia de tratamiento de los datos personales. El éxito del desarrollo transfronterizo de estos servicios depende en parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad. (6) Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través

establece la pauta básica que habrá de guiar a todos los Estados miembros en la regulación de esta materia: "Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad".

Y ya en territorio español, la propia Constitución Española de 1978 garantiza específicamente el derecho al secreto de las comunicaciones en su artículo 18.3: "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial" *(*el artículo 55 prevé la suspensión de esta protección). A esta previsión le siguen, para su desarrollo, la Ley Orgánica 4/1981, de 1 de junio, sobre los estados de alarma, excepción y sitio (artículo 18); la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria (artículo 51); la Ley Orgánica 8/2003, de 9 de julio, para la reforma concursal, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (artículo 1); la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia; el Real Decreto de 14 de septiembre de 1882, por el que se aprueba la Ley de Enjuiciamiento Criminal (artículos 579 a 588); la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (artículo 33); el Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario (artículo 47); el Real Decreto 1829/1999, de 3 de diciembre, por el que se aprueba el Reglamento por el que se regula la prestación de los servicios postales, en desarrollo de lo establecido en la Ley 24/1998, de 13 de julio, del Servicio

---

de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad".

Postal Universal y de Liberalización de los Servicios Postales (artículos 5 a 7, 12), y el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (artículos 61 a 101).

Pero hasta llegar a positivar todos estos reconocimientos expresos de las garantías que asisten a los ciudadanos en el ejercicio del derecho al secreto de las comunicaciones, y obviamente de sus restricciones, la historia se ha encargado de ir perfilando lo que hoy reconocemos como un "derecho fundamental" al secreto. Así por ejemplo, antes de darle a Francia una constitución, la Asamblea Nacional estimó necesario en 1789 redactar una "Declaración de los Derechos del Hombre y del Ciudadano", que debería formar el preámbulo de la Constitución[459] y, recogió en su artículo cuarto el límite a los derechos fundamentales: "La libertad consiste en poder hacer todo aquello que no perjudique a otro: por eso, el ejercicio de los derechos naturales de cada hombre no tiene otros límites que los que garantizan a los demás miembros de la sociedad el goce de estos mismos derechos. Tales límites sólo pueden ser determinados por la ley".

En España, la Constitución de 1869 prohibía expresamente la intervención de las comunicaciones si no lo era en virtud de una autorización judicial[460] y, la Constitución española de 1876, recoge dicha protección en similares términos[461]: "No podrá detenerse ni abrirse por la autoridad gubernativa la correspondencia confiada al correo. Todo auto de

[459] La Declaración de los derechos del hombre y del ciudadano es uno de los textos fundamentales votados por la Asamblea Nacional constituyente formada tras la reunión de los Estados Generales durante la Revolución Francesa. La base de la Declaración dio lugar a la elaboración de numerosos proyectos y, tras largos debates, el texto final fue votado el día 26 de agosto de 1789 y comienza así: "Los representantes del pueblo francés, constituidos en Asamblea nacional, considerando que la ignorancia, el olvido o el menosprecio de los derechos del hombre son las únicas causas de las calamidades públicas y de la corrupción de los gobiernos, han resuelto exponer, en una declaración solemne, los derechos naturales, inalienables y sagrados del hombre, a fin de que esta declaración, constantemente presente para todos los miembros del cuerpo social, les recuerde sin cesar sus derechos y sus deberes; a fin de que los actos del poder legislativo y del poder ejecutivo, al poder cotejarse a cada instante con la finalidad de toda institución política, sean más respetados y para que las reclamaciones de los ciudadanos, en adelante fundadas en principios simples e indiscutibles, redunden siempre en beneficio del mantenimiento de la Constitución y de la felicidad de todos".

[460] Artículo 7º de la Constitución Española promulgada el 6 de Junio de 1869: "En ningún caso podrá detenerse ni abrirse por la Autoridad gubernativa la correspondencia confiada al correo, ni tampoco detenerse la telegráfica. Pero en virtud de auto de juez competente podrán detenerse una y otra correspondencia, y también abrirse en presencia del procesado la que se le dirija por correo".

[461] Artículos 7 y 8 de la Constitución Española promulgada el 30 de Junio de 1876.

prisión, de registro de morada o de detención de la correspondencia, será motivado". Más adelante, también la Constitución Española republicana de 1931, garantiza en el artículo 32 "la inviolabilidad de la correspondencia en todas sus formas, a no ser que se dicte auto judicial en contrario". Incluso durante la Dictadura del General Franco, el Fuero de los Españoles de 1945 hace referencia al secreto de las comunicaciones, aunque no cita sus garantías: "Dentro del territorio nacional, el Estado garantiza la libertad y el secreto de la correspondencia"[462].

Es evidente que, dadas las limitadas o inexistentes circunstancias de evolución tecnológica de aquellos momentos, el secreto postal y las especiales características de este tipo de comunicaciones, centraron la protección del secreto de las comunicaciones frente al Estado en aspectos sobre todo físicos (por ejemplo, el sobre que contenía la comunicación o el sello que lo lacraba), pero hoy este concepto se extiende a toda forma de comunicación existente y, en su caso, su especial naturaleza: telefonía, correo electrónico, mensajes de texto (SMS) o multimedia, etc., en general, cualquier sistema que permita una comunicación por un canal cerrado entre dos o más personas, y esté resguardado de intromisiones de terceros no participantes de dicha comunicación.

El derecho al secreto de las comunicaciones se basa en dos conceptos básicos, la libertad y el secreto. La libertad para comunicar y el secreto de todos los aspectos de lo comunicado.

La conceptuación de este derecho ha sido tratada por diferentes corrientes doctrinales, que pueden separarse en aquellas que lo consideran subordinado al derecho a la intimidad[463], aquellas que consideran que estos dos derechos están estrechamente vinculados, aunque mantenga cada uno

[462] Artículo 13 del Fuero de los Españoles de 17 de Julio de 1945.

[463] Esta es la posición mantenida por la doctrina y la legislación estadounidense, que entiende el derecho al secreto de las comunicaciones, junto al derecho a la inviolabilidad del domicilio, como parte de la privacidad de las personas. La Cuarta Enmienda de la Constitución de los Estados Unidos, que fue ratificada el 15 de diciembre de 1791, proclama el "derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas".

su sustantividad[464] y, aquellas que los consideran de forma absolutamente independiente[465]. En una postura conciliadora, podría considerarse que el derecho a la intimidad engloba el derecho a la protección de los datos de carácter personal, el derecho a la inviolabilidad del domicilio y, el derecho al secreto de las comunicaciones, manteniendo de cada uno de ellos su propia sustantividad y, la necesitad de un reconocimiento y garantía expresa.

En principio, consideremos la jurisprudencia del Tribunal Constitucional[466] como fuente del concepto, y que señala el derecho al secreto de las comunicaciones posee su propia autonomía respecto del derecho a la intimidad, ya que los conceptos de "libertad para comunicar" y "secreto" pueden perfectamente predicarse tanto de contenidos íntimos como de contenidos no íntimos. Así lo entiende la Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre: "Ocurre, en efecto, que el concepto de "secreto" en el artículo 18.3 tiene un carácter "formal", en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado". Sin embargo, como explica el Tribunal Supremo, ambos derechos no dejan de estar vinculados precisamente por el

[464] MONTAÑÉS PARDO, M.A. y RORÍGUEZ RUÍZ, B., entre otros.

[465] MORENO CATENA, V., en su artículo "Garantía de los derechos fundamentales en la investigación penal", publicado en la Revista *Poder judicial*, bajo el título *Justicia Penal* (1987), recoge esta teoría sobre la dimensión formal del derecho al secreto de las comunicaciones (p.155), basada en que la comunicación por un canal cerrado se protege en todo caso, independientemente de que su contenido sea o no íntimo.

[466] "Este Tribunal sí ha elaborado una doctrina, ya muy consolidada, sobre el derecho al secreto de las comunicaciones telefónicas del artículo 18.3 CE. Así, a modo de resumen en la citada STC 123/2002, de 20 de mayo, F.Jº. 5º, recordamos: "hemos dicho, con palabras de la STC 114/1984, que el derecho al secreto de las comunicaciones (artículo 18.3 CE) protege implícitamente la libertad de las comunicaciones y, además, de modo expreso, su secreto. De manera que la protección constitucional se proyecta sobre el proceso de comunicación mismo cualquiera que sea la técnica de transmisión utilizada (STC 70/2002) y con independencia de que el contenido del mensaje transmitido o intentado transmitir -conversaciones, informaciones, datos, imágenes, votos, etc.- pertenezca o no al ámbito de lo personal, lo íntimo o lo reservado (STC 114/1984). El derecho al secreto de las comunicaciones protege a los comunicantes frente a cualquier forma de interceptación o captación del proceso de comunicación por terceros ajenos, sean sujetos públicos o privados (STC 114/1984)". A ello añadimos que "el fundamento del carácter autónomo y separado del reconocimiento de este derecho fundamental y de su específica protección constitucional reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación. A través de la protección del proceso de comunicación se garantiza, a su vez, el carácter reservado de lo comunicado sin levantar su secreto, de forma que es objeto de este derecho la confidencialidad tanto del proceso de comunicación mismo como del contenido de lo comunicado. Este reconocimiento autónomo del derecho no impide naturalmente que pueda contribuir a la salvaguarda de otros derechos, libertades o bienes constitucionalmente protegidos, como el secreto del sufragio activo, la libertad de opinión, ideológica y de pensamiento, de la libertad de empresa, la confidencialidad de la asistencia letrada o, naturalmente también, el derecho a la intimidad personal y familiar. En una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo" *(F.Jº 5º).* STC 281/2006 de 16 de Noviembre. (F.Jº. 3º).

hecho de que el secretismo implica siempre una expectativa de intimidad: "el hecho de cerrar una carta demuestra la voluntad de que su contenido no sea reconocido más que por la persona a quien va dirigido, y por tanto es un secreto que viola el que la abre sin el consentimiento del destinatario"[467].

Respecto al concepto constitucional de "comunicación"[468] que ha configurado el Tribunal Constitucional, podemos afirmar que se considera como un proceso de transmisión de mensajes entre personas determinadas.

Exactamente, la STC 281/2006 de 16 de noviembre, establece al respecto en el F.Jº. 3º:

"Pues bien, si el derecho al secreto de las comunicaciones (artículo 18.3 CE) constituye una plasmación singular de la dignidad de la persona y el libre desarrollo de la personalidad que son "fundamento del orden político y de la paz social" (artículo 10.1 CE), las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana; por tanto, la comunicación es a efectos constitucionales el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos. Aunque en la jurisprudencia constitucional no encontramos pronunciamientos directos sobre el ámbito objetivo del concepto constitucional de "comunicación", sí existe alguna referencia indirecta al mismo derivada del uso indistinto de las expresiones "comunicación" y "mensaje", o del uso de términos como "carta" o "correspondencia" cuando de la ejemplificación del secreto de las comunicaciones postales se trataba (STC 114/1984, de 29 de noviembre, F.Jº. 7º)".

En cualquier caso, y sea cual sea el ámbito objetivo del concepto de "comunicación", lo que es indudable es que la norma constitucional "se dirige a garantizar el "secreto", su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia "erga omnes") ajenos a la comunicación

[467] Sentencia del Tribunal Supremo de 6 de octubre de 1967 (R.J.A. 4091/1967).
[468] URBANO CASTRILLO, E. El derecho al secreto de las comunicaciones. Col. Derechos fundamentales. Ed. La Ley. Madrid, 2011. p. 237.

misma. La presencia de un elemento ajeno a aquellos entre los que media el proceso de comunicación, es indispensable para configurar el ilícito constitucional aquí perfilado"[469]. MARTÍN MORALES, añade que además de la intromisión, se prohíbe la "reproducción y o utilización de los que a través de ella se llegue a conocer, así como la retención temporal, la obstaculización o la desviación de la propia comunicación"[470].

Los titulares del derecho tienen en principio una expectativa razonable de defensa de la libre información y confidencialidad de sus comunicaciones, manteniéndose al margen a terceros mediante el secreto, pero no se va a considerar igualmente garantizado su derecho al secreto de las comunicaciones, cuando uno de los intervinientes revele parte o todo el contenido. En estos casos, se podría reconducir la protección de la conversación hacia la protección y garantía del derecho a la intimidad, dado que sobre los comunicantes pesa "un posible "deber de reserva" que -de existir- tendría un contenido estrictamente material, en razón de cual fuese el contenido mismo de lo comunicado"[471]. De la misma manera, la escucha de una conversación telefónica realizada desde las inmediaciones del espacio público donde tiene lugar, no se podrá considerar como una vulneración del secreto de las comunicaciones, si no se ha utilizado algún medio técnico o electrónico. En este caso, de nuevo, habría una posible vulneración de la intimidad de los comunicantes, pero no del secreto de las comunicaciones, dependiendo su análisis de otras circunstancias en que esto se produjera[472].

---

[469] Sentencia del Tribunal Constitucional 114/1984 (F.Jº.7º).

[470] MARTÍN MORALES, R. *El régimen constitucional del secreto de las comunicaciones*. Ed. Civitas. Madrid, 1995. p. 151.

[471] Ibídem.

[472] Íbídem. (F.Jº.7º). "Quien entrega a otro la carta recibida o quien emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera «íntima» del interlocutor, pudiesen constituir atentados al Derecho garantizado en el artículo 18.1 de la Constitución. Otro tanto cabe decir en el presente caso, respecto de la grabación por uno de los interlocutores de la conversación telefónica. Este acto no conculca secreto alguno impuesto por el artículo 18.3 y tan sólo, acaso, podría concebirse como conducta preparatoria para la ulterior difusión de lo grabado. Por lo que a esta última dimensión del comportamiento considerado se refiere, es también claro que la contravención constitucional sólo podría entenderse materializada por el hecho mismo de la difusión (artículo 18.1 de la Constitución). Quien graba una conversación de otros atenta, independientemente de otra consideración, al derecho reconocido en el artículo 18.3 de la Constitución; por el contrario, quien graba una conversación con otro no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado, si se impusiera un genérico deber de secreto a cada uno de los interlocutores o de los corresponsables ex artículo 18.3, se terminaría vaciando de sentido, en buena parte de su alcance normativo, a la protección de la esfera íntima personal ex artículo 18.1, garantía ésta que, "a contrario",

Para hablar de protección de la comunicación, en el sentido constitucional de garantizar su secreto, debe haberse realizado a través de un canal cerrado y entre comunicantes determinados, pues eso es lo que justificará la expectativa de confidencialidad que defiende la jurisprudencia, independientemente de que el contenido pertenezca al ámbito de lo personal, lo íntimo o lo reservado[473]. Pero además el secreto puede extenderse más allá del contenido de la comunicación, debería integrarse en él la protección de los llamados "datos de tráfico", como son por ejemplo la identidad de los que intervienen en la comunicación, el origen y destino, y la duración. La referida STC 114/1984, así lo reconocía cuando dice que la identidad subjetiva de los interlocutores es parte del secreto de la comunicación[474], aunque la jurisprudencia del Tribunal Supremo ahora camine por otros derroteros considerándolo meros "datos accesorios a la comunicación"[475].

En resumen, el bien jurídico protegido[476] por el artículo 18.3 CE es el proceso de comunicación mientras dura, tanto el contenido como la identidad de los comunicantes u otros aspectos externos de la misma (momento, durante, destino...), frente a cualquier interferencia no consentida ni autorizada judicialmente; pero una vez finalizado el proceso

---

no universaliza el deber de secreto, permitiendo reconocerlo sólo al objeto de preservar dicha intimidad (dimensión material del secreto, según se dijo). Los resultados prácticos a que podría llevar tal imposición indiscriminada de una obligación de silencio al interlocutor son, como se comprende, del todo irrazonables y contradictorios, en definitiva, con la misma posibilidad de los procesos de libre comunicación".

[473] Ibidem.

[474] Ibidem: "Y puede también decirse que el concepto de "secreto", que aparece en el artículo 18.3, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales. La muy reciente Sentencia del Tribunal Europeo de Derechos del Hombre de 2 de agosto de 1984 -caso Malone- (TEDH 1984\1) reconoce expresamente la posibilidad de que el artículo 8 de la Convención pueda resultar violado por el empleo de un artificio técnico que, como el llamado "comptage", permite registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma".

[475] Sentencia del Tribunal Supremo de fecha 5 de Febrero de 2008 y, Acuerdo adoptado por la Sala de lo Penal de Tribunal Supremo, con fecha 23 de Febrero de 2010.

[476] (...) "hay que recordar que el derecho al secreto de las comunicaciones es una garantía formal de la libertad para comunicarse sin interferencias. Con independencia del contenido de la comunicación, lo que se protege es el continente: la impenetrabilidad de la comunicación para terceros, ya sea un poder público o un particular. Y ello con independencia de que se trate de aspectos íntimos o reservados de la persona. Por tanto, el bien jurídico protegido es el proceso de comunicación mismo. "El juez ante las escuchas telefónicas". MARC CARRILLO. *El País*. 25 de marzo de 2010. http://elpais.com/diario/2010/03/25/opinion/1269471604_850215.html

en que la comunicación consiste, la protección constitucional sería la brindada por el artículo 18.1 CE[477].

Y las garantías constitucionales que permiten la injerencia en las comunicaciones, son:

a) Habilitación legal: una norma precisa, clara y detallada, derivada de las exigencias de seguridad jurídica y certeza, que indique bajo qué condiciones y circunstancias estarán habilitados los poderes públicos para tomar estas medidas[478].
b) Principio de proporcionalidad[479]: es límite para toda injerencia estatal en los derechos fundamentales, el que exista un fin constitucionalmente legítimo que pueda justificar la medida. Es decir, que sea estrictamente necesaria[480] y no existan medios alternativos.
c) Autorización judicial motivada: una explicación precisa de las circunstancias que hacen preciso adoptar la medida por una autoridad judicial. Se ha de justificar la existencia de los presupuestos materiales habilitantes de la intervención, o sea, los datos que objetivamente denotan la comisión de un hecho delictivo grave ("indicios") sobre la conexión de las personas afectadas por la intervención con los hechos investigados[481]. No bastan meras sospechas o decir que existe una investigación previa.
d) Control judicial de la ejecución de la medida: que se atenga a los términos de su adopción, a las personas, y a los límites temporales y/o físicos que se establezcan en la autorización[482].

[477] RODRÍGUEZ MONTAÑÉS, T. Artículo 18.3 CE: El secreto de las comunicaciones. En Comentarios a la Constitución Española... Op. Cit. pp. 442 – 455.
[478] Artículo 8 CEDH, y STC 49/1996, de 26 de Marzo (F.Jº. 3º).
[479] Ibídem (F.Jº. 7º).
[480] Ibídem (F.Jº. 8º).
[481] Ibídem.
[482] STC 166/1999, de 27 de Septiembre (F.Jº. 2º).

1.1.b.- La Directiva sobre la privacidad y las comunicaciones, y su reflejo en el derecho interno español.

La Directiva 2002/58/CE, la llamada "Directiva sobre la privacidad y las comunicaciones electrónicas", define estos datos como "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma"[483] y señala que:

> "Una comunicación puede incluir cualquier dato relativo a nombres, números o direcciones facilitado por el remitente de una comunicación o el usuario de una conexión para llevar a cabo la comunicación. Los datos de tráfico pueden incluir cualquier conversión de dicha información efectuada por la red a través de la cual se transmita la comunicación a efectos de llevar a cabo la transmisión. Los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión. También pueden referirse al formato en que la red conduce la comunicación".

Y, en su artículo 5 la Directiva aplica a estos datos igual protección que a la confidencialidad[484] de las comunicaciones, diciendo que (...) "En particular, prohibirán la escucha, la grabación, el almacenamiento u otros

[483] Artículo 2.b) ("Definiciones") de la Directiva 2002/58/CE de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

[484] Comienza el primer apartado del artículo 5 de la Directiva 2002/58/CE diciendo que: Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público.

tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad".

Por su parte, el Convenio 185 del Consejo de Europa sobre Cibercrimen, celebrado en Budapest el 23 de noviembre de 2002, precisa en su primer artículo este concepto, explicando que afecta a "todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente". Se trata en definitiva de gran parte de los datos relativos a los abonados que conservan los prestadores de servicios de comunicaciones[485].

El Grupo de Trabajo del Artículo 29 ha emitido sendos dictámenes sobre la Directiva 2002/58/CE, exponiendo su opinión respecto al marco regulador de la privacidad y las comunicaciones, que antes venía configurado por otras cuatro Directivas relativas al tratamiento de los datos personales que se realizan en comunicaciones electrónicas o, a través de comunicaciones electrónicas y su seguridad[486]. La más reciente de ellas, venía a armonizar las disposiciones contenidas en las anteriores, y sobre ello, el Grupo de Trabajo quiso hacer una serie de precisiones. El Dictamen 8/2006 sobre la revisión del marco regulador de las redes y los servicios de

[485] El artículo 18.3 del Convenio 185 del Consejo de Europa sobre Cibercrimen, celebrado en Budapest el 23 de noviembre de 2002, integra en un solo concepto tanto los datos que corresponden a la comunicación, como los que corresponden al ámbito de la intimidad de los comunicantes. – "A los efectos del presente artículo, la expresión «datos relativos a los abonados» designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido, y que permite establecer: a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio; b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y el pago, disponibles por razón de un contrato o de un alquiler de servicio; c. cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un alquiler de servicio".

[486] Directivas 19/2002/CE, Directiva 20/2002/CE, Directiva 21/2002 y Directiva 22/2002/CE.

comunicaciones electrónicas, con especial atención a la Directiva sobre la privacidad y las comunicaciones electrónicas, adoptado el 26 de septiembre de 2006, y del Dictamen 2/2008 sobre la revisión de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (Directiva sobre privacidad), emitido el 15 de mayo de 2008.

En el primero, el Dictamen 8/2006, el Grupo de Trabajo retoma una serie de propuestas que ya ofreciera en su Dictamen 7/2000 sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y, que no fueron tenidas en cuenta[487], y añade una serie de observaciones específicas sobre el Documento de trabajo de los servicios de la Comisión. Se trata mayoritariamente de cuestiones de carácter técnico[488] sobre el papel de los proveedores de servicios en materia de "seguridad", pero también se refiere a aspectos que afectan directamente a los usuarios, considerando que "en lugar de abordar la "seguridad" en su sentido más amplio, debe prestarse atención a aspectos concretos de la misma – no sólo a la "continuidad" y "confidencialidad", sino también a la "integridad" de los datos, y en especial

[487] (1) En el Dictamen mencionado, el grupo de trabajo del artículo 29 subrayaba que la solución consistente en que las disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas se apliquen únicamente a la provisión de los servicios de comunicaciones electrónicos públicamente disponibles en las redes de comunicación públicas no era muy afortunada porque las redes privadas están adquiriendo una importancia cada vez mayor en la vida cotidiana y los riesgos que esas redes plantean para la protección de la intimidad están consecuentemente aumentando, en especial porque tales redes son cada vez más específicas (por ejemplo, control del comportamiento de los empleados a través del tráfico de datos). Otro factor que aboga por la reconsideración del ámbito de aplicación de la Directiva es la tendencia de los servicios a convertirse en una mezcla de servicios privados y públicos. (2) El grupo de trabajo del artículo 29 observa que tanto la definición de "servicios de comunicaciones electrónicas" como la de "proveedor de una red de comunicaciones electrónica" no son aún lo suficientemente claras, por lo que habría que precisarlas para que tanto los reguladores como los usuarios de los datos puedan interpretarlas clara e inequívocamente. Esas definiciones poco claras suscitan varias cuestiones como, por ejemplo, ¿se puede considerar un cibercafé como proveedor de una red de comunicaciones electrónica? Aunque este tipo de preguntas deberían ser fáciles de contestar, no siempre sucede así. (3) Además, el grupo de trabajo del artículo 29 en su Dictamen 7/2000 hacía referencia al considerando nº 25 de la Directiva sobre la privacidad y las comunicaciones electrónicas relativo al uso de "chivatos" (cookies). En ese considerando se dice que los usuarios deben tener la posibilidad de impedir que se almacene en sus ordenadores personales un "chivato" (cookie). El grupo de trabajo del artículo 29 apoyó completamente este punto de vista. Sin embargo, la última frase del considerando nº 25, en la que se afirma que se podrá supeditar el acceso a determinados contenidos de un sitio web a la aceptación fundada de un "chivato", en caso de que éste tenga un propósito legítimo, puede estar en contradicción con la afirmación de que los usuarios deben tener la posibilidad de impedir el almacenamiento de un "chivato" en sus ordenadores personales y por lo tanto puede requerir una aclaración o revisión".

[488] "Prever los posibles cometidos específicos de los proveedores de infraestructuras de acceso y de los proveedores de servicios, puede resultar de interés a la hora de determinar si es necesario reforzar la reglamentación sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas, para evitar cualquier malentendido sobre los destinatarios de esa reglamentación. Por lo tanto la propuesta legislativa debe aportar claridad y no crear más confusión".

a las cuestiones relacionadas con la dicotomía autentificación/anonimato", y apuesta por introducir un apartado específico sobre el "fraude de identidad", en el que se podría decir que "tanto la confidencialidad como la supresión oportuna de datos personales excesivos contribuyen a combatir la usurpación de identidad"[489].

En general en este Dictamen, el Grupo de Trabajo viene a exponer que "si bien apoya la mejora de las medidas de seguridad, no apoya ninguna medida que lleve o pueda llevar a incrementar la vigilancia o a bloquear los contenidos, y recomienda:

> 1.- la mejora de las medidas de seguridad y subraya que la protección de los usuarios y la forja de la confianza de éstos en las comunicaciones electrónicas se deben tener muy en cuenta al tiempo que se mejora la seguridad de las infraestructuras.
>
> 2.- que se aborden los temas relacionados con las aplicaciones en línea, entre los que se incluyen cuestiones de seguridad, la responsabilidad de los operadores así como una aclaración de la personalidad jurídica tanto de los proveedores de infraestructuras de acceso y de los proveedores de servicios como de los responsables del tratamiento de datos".

El Dictamen 2/2008, se emitió sobre la base de una propuesta de Directiva que modificaría, entre otras cosas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, adoptada por la Comisión Europea con fecha 13 de noviembre de 2007.

De dicha propuesta destaca el Grupo de Trabajo el esfuerzo por reforzar la seguridad en las redes de comunicación con previsiones que

[489] Pero continúa diciendo: "Sin embargo, al abordar temas de autentificación, hay que tener en cuenta que, en principio, los individuos deben poder utilizar anónimamente los servicios electrónicos públicos. Por lo tanto, antes de realizar cualquier propuesta o modificación que se refiera a cuestiones de autentificación debe llevarse a cabo un concienzudo análisis de la accesibilidad de los servicios electrónicos, puesto que la comunicación libre es fundamental".

obliguen a los proveedores a informar sobre las vulneraciones de seguridad que se produzcan, cuando afecten a servicios de la sociedad de la información. Además, "se felicita de que la definición y el ámbito del término "datos personales" de la propuesta sean totalmente compatibles con la definición correspondiente de la Directiva sobre protección de datos, y subraya que cualquier restricción del ámbito de esta definición en la Directiva sobre privacidad crearía una diferencia en la protección de las personas en un campo que está en el centro de las comunicaciones electrónicas –y por lo tanto también de los servicios de la sociedad de la información y de administración en línea (eGovernment) basados en servicios electrónicos–, y sería pues totalmente inaceptable desde el punto de vista de la protección de la privacidad".

Además, añade una previsión de mejora de la protección de la privacidad de las personas por la vía judicial, recomendando que "se permita una vía de recurso legal en caso de infracción de disposiciones nacionales que prohíban el uso del programas espía (spyware)" y, por otra parte, recuerda que es preceptivo "garantizar la confidencialidad de las comunicaciones con independencia de la naturaleza de la red y de si las comunicaciones cruzan las fronteras de la UE", y recomienda que los proveedores de servicios de comunicaciones electrónicas redoblen los esfuerzos para "proteger mejor a todas las personas que mantienen comunicaciones electrónicas en las que toman parte terceros de países no comunitarios"[490].

Por último, subrayar la referencia expresa que hace a las direcciones IP, en materia de telecomunicaciones, como dato de carácter personal:

> "El Grupo de Trabajo del Artículo 29 observa que en el debate sobre la Directiva sobre privacidad se ha planteado si las direcciones IP son datos personales. El Grupo de Trabajo del Artículo 29 recuerda que, en la mayoría de los casos (incluso

[490] "La revisión de la Directiva sobre privacidad es el foro oportuno para afirmar los derechos civiles en este aspecto y, en especial, para garantizar la transparencia en los mecanismos utilizados para la conducción de comunicaciones".

> en los casos de asignación de dirección IP dinámica), se dispondrá de los datos necesarios para identificar al/los usuario(s) de la dirección IP. El Grupo de Trabajo ya observó en su Dictamen WP 1366 que (...) "a menos que el prestatario de servicios de Internet sepa con absoluta certeza que los datos corresponden a usuarios que no pueden ser identificados, tendrá que tratar toda información IP como datos personales, para guardarse las espaldas". Estas consideraciones se aplicarán igualmente a los operadores de motores de búsqueda (WP 1487)".

Como hemos visto, en Europa, y por mandato implícito en España, tanto la normativa específica en materia de telecomunicaciones, como la doctrina, seguida de la jurisprudencia, se han preocupado de delimitar el concepto de "derecho al secreto de las comunicaciones" y las garantías que le asisten, y lo han hecho centrándose principalmente en definir qué se entiende por "secreto", de tal forma que cualquier injerencia en la esfera que se protege, deba estar justificada en todo caso por una ley y/o una autorización judicial que determine el interés legítimo que justifique levantar ese secreto en sacrificio del propio derecho. Debe realizarse una valoración de la proporcionalidad, y de la necesidad en un Estado democrático, de tal medida.

Las posibilidades de restringir, suspender o vulnerar el derecho al secreto de las comunicaciones de forma lícita son excepcionales, y están perfectamente tasadas en las leyes españolas aunque no con la precisión que debiera[491], dado el carácter fundamental de este derecho, como se verá más adelante.

[491] Asunto Prado Bugallo contra España, Sentencia TEDH de 18 febrero 2003, sobre el derecho al respeto a la vida privada y familiar. Esta Sentencia condena a España en relación con un asunto de escuchas telefónicas, y pone de relieve las carencias de las garantías legislativas, citando jurisprudencia como el asunto Valenzuela Contreras contra España, y Castillo Algar contra España, ambas de 1998, por violación del artículo 8 del CEDH. Entiende que dichas garantías no responden a todas las condiciones fijadas por la jurisprudencia del TEDH, en particular, la fijación de los límites temporales y de las condiciones de aportación de la prueba al juicio oral. Es España, a consecuencia de estas resoluciones, el el Tribunal Constitucional reconoció en su Sentencia 184/2003, de 23 de octubre, la insuficiencia del artículo 579 LECrim., en relación con el plazo máximo de duración de las intervenciones, la naturaleza y gravedad de los hechos en virtud de cuya investigación pueden acordarse; el control del resultado de las intervenciones telefónicas y de los soportes en los que conste dicho resultado, y las condiciones de incorporación a los atestados y al proceso de las conversaciones intervenidas. Entiende que el Alto

Por una parte, las situaciones más excepcionales vienen dadas por el artículo 116 de la Constitución Española, y en su desarrollo, por la Ley Orgánica 4/1981, de 1 de junio, de los Estados de Alarma, Excepción y Sitio, que permite la suspensión de determinados derechos fundamentales, en circunstancias de especial gravedad para la estabilidad del Estado. Entre otros, se prevé la suspensión del derecho al secreto de las comunicaciones.

Por otra parte, el artículo 55 de la Constitución Española, dentro del Capítulo 5, dedicado a la Suspensión de los Derechos y Libertades, señala la "Ley Orgánica" como habilitadora para la suspensión:

> "1. Los derechos reconocidos en los artículos 17, 18, apartados 2 y 3; artículos 19, 20, apartados 1, a y d, y 5, artículos 21, 28, apartado 2, y artículo 37, apartado 2, podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución. Se exceptúa de lo establecido anteriormente el apartado 3 del artículo 17 para el supuesto de declaración de estado de excepción.
>
> 2. Una Ley Orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. La utilización injustificada o abusiva de las facultades reconocidas en dicha Ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las Leyes".

Y otra norma esencial que prevé la suspensión del derecho al secreto de las comunicaciones, es el artículo 579 de la Ley de

---

Tribunal este precepto por si solo no cumple con las exigencias de previsibilidad y certeza en el ámbito del derecho fundamental al secreto de las comunicaciones e insta al legislador para que en el plazo más breve posible regule con la suficiente precisión esta materia.

Enjuiciamiento Criminal, señala al Juez como habilitador de la restricción del derecho. Establece que[492]:

> "1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.
>
> 2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.
>
> 3. De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.
>
> 4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación".

[492] Redacción según Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal.

En principio, circunstancias especiales, una Ley Orgánica y/o una orden judicial, son los presupuestos básicos habilitadores de toda limitación lícita al ejercicio del derecho al secreto de las comunicaciones.

En el caso de declararse un estado de alarma, de sitio o de excepción, la suspensión tendrá que venir prevista expresamente en el decreto que declare el estado de excepción[493] y "se establece que la suspensión de este derecho sólo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público"[494]. Pero incluso en estos supuestos excepcionales se mantiene la garantía judicial, quedando a salvo la posibilidad de que cualquiera de estos actos sea llevado a la jurisdiccional[495], llegando incluso a poder plantearse un Recurso de Amparo ante el Tribunal Constitucional.

En lo que se refiere a la investigación de bandas armadas o elementos terroristas o rebeldes, el segundo párrafo del artículo 55 del CE prevé la posibilidad de suspender el derecho al secreto de las comunicaciones, pero siempre de forma individual y con la necesaria intervención judicial.

Sucede sin embargo que no siempre se logra mantener el preceptivo equilibrio entre la eficacia de la adopción de estas medidas y el fin perseguido, para luchar contra la grave amenaza del terrorismo en nuestro país. En general podría pensarse que es en la práctica dónde se ofrece un mayor riesgo por abusos contra las libertades y los derechos de las personas en estas situaciones, pero lo que es cierto es que el desarrollo

[493] El primer párrafo del artículo 55 de la Constitución Española establece que los derechos reconocidos en el artículo 18, apartados 2 y 3, entre otros, "podrán suspendidos cuando se acuerde la declaración del estado de excepción o de sitio". Nada de esto se prevé en cambio para el estado de alarma.

[494] Artículo 18 de la Ley Orgánica 4/1981, de 1 de junio, de los Estados de Alarma, Excepción y Sitio, para el estado de excepción: "Cuando la autorización del Congreso comprenda la suspensión del artículo 18.3, de la Constitución, la Autoridad Gubernativa podrá intervenir toda clase de comunicaciones, incluidas las postales, telegráficas y telefónicas. Dicha intervención solo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público. La intervención decretada será comunicada inmediatamente por escrito motivado al juez competente".

[495] Artículo 3 de la Ley Orgánica 4/1981: "Quienes como consecuencia de la aplicación de los actos y disposiciones adoptadas durante la vigencia de estos estados sufran, de forma directa, o en su persona, derechos o bienes, daños o perjuicios por actos que no les sean imputables, tendrán derecho a ser indemnizados de acuerdo con lo dispuesto en las Leyes".

legislativo de la ejecución de la suspensión de los derechos, ha planteado en distintas ocasiones muy dudosas situaciones de legitimidad en la restricción del derecho al secreto de las comunicaciones.

1.1.c.- Jurisprudencia.

La citada Sentencia del TEDH, de 18 febrero 2003, en el Asunto Prado Bugallo contra España, incide directamente en la interpretación de la normativa española, en cuanto a las deficiencias del artículo 579 de la Ley de Enjuiciamiento Criminal, respecto a la fijación de los límites temporales y de las condiciones de aportación de la prueba al juicio oral. Y en este sentido, sigue la estela de la Sentencia del TEDH, de 30 de julio de 1998, en el asunto Valenzuela Contreras contra España (precursora de la anterior, del asunto Prado Burgallo), que ponía de relieve las deficiencias de dicha regulación, tales como la previsibilidad y la accesibilidad de los supuestos en que las injerencias por las autoridades públicas están previstas. La exigencia de previsibilidad implica en todo caso que el derecho interno utilice términos suficientemente claros para marcar en qué circunstancias, o en qué condiciones, se habilita el poder público a adoptar este tipo de medidas. Esta resolución manifestaba que, para evitar abusos, deberían figurar expresamente recogidos en la ley tanto la definición de "personas susceptibles de ser sometidas a escuchas judiciales", como la naturaleza de las infracciones que pueden dar lugar a ella. También debería contener otros detalles como la fijación de un límite de la duración de la ejecución de la medida, las condiciones de establecimiento de los procedimientos verbales de síntesis consignando las conversaciones interceptadas, las precauciones a tomar para comunicar las grabaciones realizadas sin alteraciones y, las circunstancias en las que corresponda su archivo destrucción.

Por otra parte, en el asunto Kopp contra Suiza[496], el TEDH incidió en el significado de "prevista por ley", señalando que no significa sólo que la medida tenga una base en el derecho interno, sino que reflejan la cualidad de la ley en causa, señalando, que no sólo debe ser "accesible al justiciable y previsible", sino que además debe ser lo suficientemente precisa como para que su apreciación no deje margen a múltiples e incongruentes interpretaciones, debe permitir saber con bastante claridad el alcance de las medidas susceptibles de ser adoptadas[497].

Las normas dictadas en España, con posterioridad a la STDH del asunto Valenzuela Contreras, tomaron buena cuenta de sus críticas y se esforzaron por delimitar dichos supuestos, aunque no siempre con el mismo acierto, pues en la actualidad el artículo 33 de la Ley General de Telecomunicaciones regula ciertas cuestiones (que se desarrollan mediante Reglamento), sin ser Ley Orgánica, que podrían ser calificadas como restricciones a un derecho fundamental, como es la intervención de los llamados "datos de tráfico", y que se tratará en el correspondiente apartado.

De la jurisprudencia constitucional habida en España, destacan la Sentencia del TC 171/1999, de 27 de septiembre de 1999 y la Sentencia del TC 184/2003, de 23 de octubre de 2003.

La primera de estas resoluciones, cita muchas otras sentencias dictadas por el Tribunal Constitucional en esta materia[498] y, las resoluciones más relevantes hasta ese momento, del Tribunal Europeo de Derechos Humanos, algunas de las cuales ya se han citado[499], para reforzar el argumento de que una medida restrictiva del derecho al secreto de las comunicaciones sólo puede entenderse constitucionalmente legítima si está legalmente prevista con suficiente precisión, si se autoriza por autoridad

[496] Sentencia TEDH, de 25 de marzo de 1998.
[497] Asunto Calogero Diana contra Italia, Sentencia TEDH de 15 de noviembre de 1996.
[498] Sentencias del TC nº 85/1994, nº 86/1995, nº 181/1985, nº 49/1996, nº 54/1996, nº 81/1998, nº 121/1998, nº 151/1998 y, nº 49/1999.
[499] Sentencias del TEDH, asuntos Klass contra Alemania (Sentencia 6 de septiembre de 1978), Malone contra el Reino Unido (Sentencia 2 de agosto de 1984), Kruslin y Huvig contra Francia (Sentencia 24 de abril de 1990), Halford contra Reino Unido (Sentencia 25 de marzo de 1998), Kopp contra Suiza (Sentencia 25 de marzo de 1998) y Valenzuela contra España (Sentencia 30 de julio de 1998).

judicial en el marco de un proceso y, en tercer lugar, si se realiza con estricta observancia del principio de proporcionalidad[500]. Es decir, se precisa comprobar si la medida se autoriza por ser necesaria para alcanzar un fin constitucionalmente legítimo, como por ejemplo la defensa del orden y prevención de delitos calificables de delitos graves; si es adecuada e imprescindible para su investigación y, si existen indicios sobre el hecho constitutivo de delito y sobre la conexión con el mismo de las personas investigadas.

La segunda de las resoluciones, la Sentencia del TC 184/2003, de 23 de octubre de 2003, continúa la referida jurisprudencia del Tribunal Europeo de Derechos Humanos (que exige la previsión legal de las medidas limitativas de los derechos reconocidos en el Convenio Europeo de Derechos Humanos[501]), y lo hace específicamente en relación con la adopción de medidas consistentes en la interceptación de las comunicaciones y su incidencia sobre otros derechos fundamentales. En lo que se refiere específicamente a las comunicaciones telefónicas el Tribunal Europeo de Derechos Humanos ha declarado expresamente que la falta de previsión legal es una vulneración del artículo 8 CEDH, si se procede a la intervención de las comunicaciones telefónicas[502] y, que el artículo 579 de la Ley de Enjuiciamiento Criminal no satisface los requisitos necesarios exigidos por el artículo 18.3 de la CE para la protección del derecho al secreto de las comunicaciones, de acuerdo con los apartados primero y segundo del artículo 8 CEDH, ya que por ejemplo resultaba insuficiente su previsión sobre el plazo máximo de duración de las intervenciones, puesto que no determina un límite de las prórrogas que se pueden acordar; sobre la determinación de la naturaleza y gravedad de los hechos en virtud de cuya investigación pueden acordarse y, también sobre el control del resultado de las intervenciones telefónicas y de los soportes en los que conste dicho

[500] STC 49/1999, F.Jº. 4º, 6º y 7º.

[501] Sentencias del TEDH, asuntos Sunday Times contra el Reino Unido (Sentencia 26 de abril de 1979), Piermont contra Francia (Sentencia 27 de abril de 1995), Rekveny contra Hungría (Sentencia de 20 de mayo de 1999), Hashman y Harrup contra el Reino Unido (Sentencia de 25 de noviembre de 1999), Demirtepe contra Francia (Sentencia 21 de diciembre de 1999), Rinzivillo contra Italia (Sentencia 21 de diciembre de 2000), Di Giovine contra Italia (Sentencia 26 de julio de 2001) y Messina contra Italia (Sentencia 24 de octubre de 2002).

[502] Sentencias del TEDH, asuntos Amann c. Suiza (Sentencia 16 de febrero de 2000), Rotaru c. Rumania (Sentencia 4 de mayo de 2000), P. G. y J. H. contra Reino Unido (Sentencia 25 de septiembre de 2001), a las que han de añadirse las dos citadas Sentencias Valenzuela c. España y Prado Bugallo c. España.

resultado (las condiciones de grabación, y custodia, utilización y borrado de las grabaciones, y las condiciones de incorporación a los atestados y al proceso de las conversaciones intervenidas)[503].

Alude además a la STC 49/1999, de 5 de abril (F.Jº. 5º), donde decía que dichas exigencias se concretan en: "la definición de las categorías de personas susceptibles de ser sometidas a escucha judicial; la naturaleza de las infracciones susceptibles de poder dar lugar a ella; la fijación de un límite a la duración de la ejecución de la medida; el procedimiento de transcripción de las conversaciones interceptadas; las precauciones a observar, para comunicar, intactas y completas, las grabaciones realizadas a los fines de control eventual por el Juez y por la defensa; las circunstancias en las cuales puede o debe procederse a borrar o destruir las cintas, especialmente en caso de sobreseimiento o puesta en libertad". Y es que como ya se ha dicho, tampoco regula expresamente y, por tanto, con la precisión requerida por las exigencias de previsibilidad de la injerencia en un derecho fundamental las condiciones de grabación, custodia y utilización frente a ellos en el proceso penal como prueba de las conversaciones grabadas de los destinatarios de la comunicación intervenida, pues el artículo 579 de la ley de Enjuiciamiento Criminal sólo habilita para afectar el derecho al secreto de las comunicaciones de las "personas sobre las que existan indicios de responsabilidad criminal en el momento de acordar la intervención de las comunicaciones telefónicas de las que sean titulares o de las que se sirvan para realizar sus fines delictivos", pero no habilita expresamente la afectación del derecho al secreto de las comunicaciones de los terceros con quienes aquéllos se comunican.

Le corresponde en todo caso al legislador ponderar la proporcionalidad de la exclusión, o inclusión, de determinadas personas o grupos de personas, y en su caso bajo qué requisitos, en atención a la eventual afección de otros derechos fundamentales concurrentes al intervenirse sus comunicaciones (o las de aquellos con quienes se comunican), como en el caso de Abogados o profesionales de la información

[503] "Por ello, hemos de convenir en que el artículo 579 LECrim no es por sí mismo norma de cobertura adecuada, atendiendo a las garantías de certeza y seguridad jurídica, para la restricción del derecho fundamental al secreto de las comunicaciones telefónicas (artículo 18.3 CE)".

el derecho al secreto profesional[504], o en el caso de Diputados o Senadores el derecho al ejercicio de su cargo de representación política[505], su inmunidad parlamentaria y la prohibición de ser inculpados o procesados sin previa autorización de la Cámara respectiva[506].

Y es que, tal y como insiste la Sentencia 49/1999, de 5 de abril, en su F.Jº. 4º: "por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (artículo 81.1 CE), o limite o condicione su ejercicio (artículo 53.1 CE), precisa una habilitación legal". Es decir, que la injerencia en los derechos fundamentales sólo puede ser habilitada por la "ley" en sentido estricto, lo que "implica condicionamientos en el rango de la fuente creadora de la norma y en el contenido de toda previsión normativa de limitación de los derechos fundamentales[507].

Un supuesto específico de previsión legal lo constituye la suspensión del ejercicio del derecho al secreto de las comunicaciones contenido en la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria.

El artículo 25.2 de la Constitución Española señala que en principio, un condenado a pena de prisión, que estuviere cumpliendo la misma gozará de todos los derechos fundamentales recogidos en la CE, "a excepción de los que se vean expresamente limitados por el contenido del fallo condenatorio, el sentido de la pena y la Ley penitenciaria", lo que significa que el derecho al secreto de las comunicaciones puede verse alterado por las particularidades del caso concreto de internamiento en un establecimiento penitenciario ante el que nos encontremos, pero que en todo caso, habrán de ser ordenado por un juez ponderando los intereses en juego.

---

[504] Artículos 24.2, párrafo 2, y 20.1.d de la Constitución Española.
[505] Artículo 23. 2 de la Constitución Española.
[506] Artículo 71. 2 de la Constitución Española.
[507] Sentencia del TC 169/2001, de 16 de julio (F.Jº. 6º) y, respecto al derecho a la intimidad, Sentencias nº 37/1989, de 15 de febrero (F.Jº. 7º); nº 207/1996, de 16 de febrero (F.Jº. 4º) y, nº 70/2002, de 3 de abril (F.Jº. 10º).

El desarrollo de la Ley Orgánica 1/1979, de 26 de septiembre[508], se lleva a cabo por el Reglamento Penitenciario, en cuyo artículo 46 se señala, en los últimos apartados que:

> "5. En los casos en que, por razones de seguridad, del buen orden del establecimiento o del interés del tratamiento, el Director acuerde la intervención de las comunicaciones escritas, esta decisión se comunicará a los internos afectados y también a la autoridad judicial de que dependa si se trata de detenidos o presos, o al Juez de Vigilancia si se trata de penados. Cuando el idioma utilizado no pueda ser traducido en el establecimiento, se remitirá el escrito al centro directivo para su traducción y curso posterior.
>
> 6. Las comunicaciones escritas entre los internos y su Abogado defensor o Procurador sólo podrán ser intervenidas por orden de la autoridad judicial. No obstante, cuando los internos tengan intervenidas las comunicaciones ordinarias y se dirijan por escrito a alguna persona manifestando que es su Abogado defensor o Procurador, dicha correspondencia se podrá intervenir, salvo cuando haya constancia expresa en el expediente del interno de que dicha persona es su Abogado o Procurador, así como de la dirección del mismo.

[508] Artículo 51 de la Ley Orgánica 1/1979, de 26 de septiembre.
"1. Los internos autorizados para comunicar periódicamente, de forma oral y escrita, en su propia lengua, con sus familiares, amigos y representantes acreditados de organismos e instituciones de cooperación penitenciaria, salvo en los casos de incomunicación judicial. Estas comunicaciones se celebrarán de manera que se respete al máximo la intimidad y no tendrán más restricciones, en cuanto a las personas y al modo, que las impuestas por razones de seguridad, de interés de tratamiento y del buen orden del establecimiento.
2. Las comunicaciones de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales y con los procuradores que lo representen, se celebrarán en departamentos apropiados y no podrán ser suspendidas o intervenidas salvo por orden de la autoridad judicial y en los supuestos de terrorismo.
3. En los mismos departamentos podrán ser autorizados los internos a comunicar con profesionales acreditados en lo relacionado con su actividad, con los asistentes sociales y con sacerdotes o ministros de su religión, cuya presencia haya sido reclamada previamente. Estas comunicaciones podrán ser intervenidas en la forma que se establezca reglamentariamente.
4. Las comunicaciones previstas en este artículo podrán efectuarse telefónicamente en los casos y con las garantías que se determinen en el Reglamento.
5. Las comunicaciones orales y escritas previstas en este artículo podrán ser suspendidas o intervenidas motivadamente por el director del establecimiento, dando cuenta a la autoridad judicial competente".

7. La correspondencia entre los internos de distintos centros penitenciarios podrá ser intervenida mediante resolución motivada del Director y se cursará a través de la Dirección del establecimiento de origen. Efectuada dicha intervención se notificará al interno y se pondrá en conocimiento del Juez de Vigilancia. Estas intervenciones se limitarán exclusivamente a la correspondencia entre internos sin que afecte al resto de las comunicaciones escritas*".*

En cualquier caso, siempre habrán de ponderarse todas y cada una de las circunstancias concurrentes tanto del propio centro de internamiento, de la seguridad de las instalaciones, así como de la naturaleza del interno y el peligro potencial que suponga mantener el ejercicio del derecho mientras se encuentra internado[509], pero al margen de todo esto, las garantías deberán seguir las pautas generales antes señaladas: especial motivación, limitación temporal estrictamente necesaria y comunicación al juez, y en este sentido, el Tribunal Constitucional, en la Sentencia 73/1983, de 30 de julio, se refería a la necesidad de que se respetase al máximo el derecho a la intimidad en las comunicaciones entre los internos y que, con carácter general, las comunicaciones sólo pudieran ser suspendidas por orden judicial, "si bien en los supuestos de terrorismo además podrá acordar la suspensión el Director del establecimiento, dando cuenta a la autoridad judicial competente" (F.Jº. 7º). La jurisprudencia constitucional además recuerda que esta circunstancia ha de notificarse al interno puesto que se trata de una medida con finalidad preventiva y no, para la investigación de posibles delitos[510] y que, del control de que todo ello se haga con las debidas garantías, ha de encargarse el juez de vigilancia penitenciaria.

[509] Por ejemplo, se estima conforme a derecho la intervención de las comunicaciones escritas de un interno acordada por la Dirección del Centro penitenciario por razones de seguridad del Centro, teniendo en cuenta la organización terrorista a la que pertenece el interno, en las Sentencias del TC nº 106/2001, de 23 de abril , nº 192/2002, nº 193/2002 y nº 194/2002, de 28 de octubre. También se encuentra una referencia similar en el Auto de la Audiencia Provincial de Cantabria, de 15 de febrero de 2001.
[510] Sentencia TC 200/1997, de 24 de noviembre.

1.1.d.- Vulneración del secreto por agentes públicos.

Hasta aquí se han puesto de relieve los supuestos más característicos de suspensión de las garantías del ejercicio del derecho al secreto de las comunicaciones por los poderes públicos y, sobre todo, los requisitos que ineludiblemente se han de cumplir para ello. Pero, nada se ha dicho sobre las limitaciones arbitrarias o las injerencias ilícitas que vulneran la confidencialidad de las comunicaciones.

En el sentido material, para hablar de ese tipo de vulneraciones debemos retomar el concepto de "secreto", pues es el conocimiento o la revelación del contenido de la comunicación lo que va a marcar la naturaleza de la lesión al derecho, aunque sea puesto en conexión con otras circunstancias que también puedan afectar negativamente al proceso de la comunicación, como por ejemplo la aprehensión física del mensaje, el impedimento de la comunicación en si[511] o, como ya se ha señalado, la interceptación de los datos de tráfico "por terceros ajenos a la comunicación misma"[512].

Es evidente que los particulares pueden efectuar intromisiones en el derecho al secreto de las comunicaciones, y en estos supuestos hay que estar a lo dispuesto por la Ley Orgánica 1/1982, de 5 de mayo, de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen, cuyo artículo 2 recoge aquellos supuestos que "tendrán la consideración de intromisiones ilegítimas en el ámbito de protección" de dicha ley, y entre otros, cita expresamente "la utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción". Y, ante tales situaciones, se debe

[511] Asunto Golder contra el Reino Unido, de 21 de febrero de 1975.
[512] Asunto Malone contra el Reino Unido, de 2 agosto 1984 y, Sentencia TC 114/1984 (F.Jº.7º).

acudir a la protección que ofrece el Código Penal en su artículo 197, cuando la intromisión es realizada por personas físicas y, en su artículo 200, cuando lo es por personas jurídicas[513]. Estos delitos sólo serán perseguibles a instancia de parte (artículo 201 CP: "será necesaria denuncia de la persona agraviada o de su representante legal"), salvo que afecten a intereses generales o a una pluralidad de personas.

Pero en la materia que nos ocupa, revisten especial interés las posibles vulneraciones provocadas por los agentes públicos, porque suelen quedar como cuestiones de "materia reservada" o "información clasificada", al provenir de complejos programas gubernativos de espionaje, puestos en marcha por las agencias como la Agencia Nacional de Seguridad norteamericana (NASA), la Oficina Central de Comunicaciones del Gobierno británico (GCHQ), el Servicio de Información Federal alemán (BND), la Dirección General de Seguridad Exterior francesa (DGSE) o, en España, el Centro Nacional de Inteligencia (CNI), creado en virtud de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia y, cuya principal misión "la de proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier riesgo o amenaza que afecte a la

[513] Artículo 197 CP.
"1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.
4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.
5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.
6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años".
Artículo 200 CP.
"Lo dispuesto en este Capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código".

independencia e integridad de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones"[514]. Aunque desde el TDEH se han criticado estas operaciones y se ha advertido de la necesidad del control judicial de estas operaciones, de "garantías suficientes contra los abusos, ya que un sistema de vigilancia secreta destinado a proteger la seguridad nacional crea el riesgo de minar, o incluso de destruir, la democracia pretendiendo defenderla"[515].

En el ámbito policial, la Sentencia del Tribunal Constitucional 166/1999, de 27 de setiembre de 1999, marca los límites que deben tenerse en cuenta en la ejecución de una intervención de comunicaciones, hace un repaso a los requisitos y circunstancias que harían que dicha intervención se convirtiese en una vulneración de derechos fundamentales por parte de un agente público.

> "En consecuencia, como ha sido expuesto en la STC 121/1998, F.Jº. 5º (ratificado en la STC 151/998, F.Jº. 4º), la intervención de las comunicaciones telefónicas puede constituir una vulneración del derecho al secreto de las comunicaciones si no se respetan las garantías constitucionales a él inherentes en alguna de las fases diferenciables en el curso de la misma: en primer lugar, en la decisión de intervención, en segundo lugar, en su ejecución policial, y, en tercer lugar, en el control judicial de la ejecución. (F.Jº. 3º)".

Son tres las fases que se distinguen: decisión, ejecución y, control judicial. En función de la fase ante la que nos encontremos las vulneraciones del derecho fundamental podrán adoptar una u otra forma, pero en todo caso, la medida debe estar prevista con precisión por una ley, autorizada judicialmente en el marco de una investigación penal, y ha de ser

[514] Exposición de Motivos de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
[515] Sentencia del TEDH Klass y otros contra Alemania, de 6 de septiembre de 1978 y, la Sentencia del TEDH Leander contra Suecia, de 25 de febrero de 1987.

proporcionada a los fines que se busca conseguir con ello[516]. En este sentido, dice la referida sentencia que "la proporcionalidad implica, además, de un lado, que la medida solo puede ser adoptada por resolución judicial que exprese la ponderación exigida por el juicio de necesidad en atención a los fines legítimos y a las circunstancias concretas concurrentes en cada momento (SSTC 160/1994, 50/1995, 181/1995, 49/1996, 54/1996, F.Jº 7º y 8º); de otro, que la ejecución de la misma debe atenerse a los estrictos términos de la autorización, tanto en cuanto a los límites materiales o temporales de la misma como a las condiciones de su autorización (SSTC 85/1994, F.Jº. 3º, 86/1995, F.Jº. 3º, 49/1996, F.Jº. 3º, 121/1998, F.Jº. 5º); y, finalmente, que la medida debe ser verificada bajo control judicial (por todas SSTC 49/1996, F.Jº. 3º, 121/1998, F.Jº. 5º, 151/1998, F.Jº. 4º)".

En el momento de tomar la decisión de intervenir una comunicación, se puede incurrir en una ilicitud si no interviene un órgano jurisdiccional, si no se ciñe a la previsión legal que la habilita y los requisitos que establece para ello y, si no existe en curso una investigación "por un hecho constitutivo de infracción punible grave, en atención al bien jurídico protegido y a la relevancia social del mismo, y en la existencia de indicios sobre el hecho constitutivo de delito y sobre la conexión con el mismo de las personas investigadas"[517]. Es decir, si no se dan los presupuestos básicos que

[516] STC 166/1999, de 27 de septiembre. (F.Jº.2º): "De la síntesis de la jurisprudencia constitucional (SSTC 114/1984, 85/1994, 86/1995, 181/1985, 49/1996, 54/1996, 81/1998, 121/1998, 151/1998, 49/1999) y del Tribunal Europeo de Derechos Humanos --casos Klass (Sentencia 6 de septiembre de 1978), Malone (Sentencia 2 de agosto de 1984), Kuslin y Huvig (Sentencia 24 de abril de 1990), Haldford (Sentencia 25 de marzo de 1998), Klopp (Sentencia 25 de marzo de 1998) y Valenzuela (Sentencia 30 de julio de 1998)--, deriva que una medida restrictiva del derecho al secreto de las comunicaciones sólo puede entenderse constitucionalmente legítima desde la perspectiva de este derecho fundamental si, en primer lugar, está legalmente prevista con suficiente precisión --principio de legalidad formal y material (STC 49/1999, F.Jº. 4º); si, en segundo lugar, se autoriza por autoridad judicial en el marco de un proceso (STC 49/1999, F.Jº. 6º); y si, en tercer lugar, se realiza con estricta observancia del principio de proporcionalidad (STC 49/1999, F.Jº. 7º); es decir, si la medida se autoriza por ser necesaria para alcanzar un fin constitucionalmente legítimo, como --entre otros--, para la defensa del orden y prevención de delitos calificables de infracciones punibles graves, y es idónea e imprescindible para la investigación de los mismos (ATC 344/1990, SSTC 85/1994, F.Jº. 3º, 181/1995, F.Jº. 5º, 49/1996, F.Jº. 3º, 54/1996, fundamentos jurídicos 7º y 8º, 123/1997, F.Jº. 4º; SSTEDH casos Huvig y Kruslin, y Valenzuela)".

[517] Ibídem (F.J. 3º) "La decisión de intervención puede ser ilegítima, en primer término, por no haber sido adoptada por órgano judicial (por todas STC 86/1995, F.Jº. 3º); en segundo lugar, por inexistencia de los presupuestos materiales que habilitan legal y constitucionalmente para la adopción de la decisión judicial de intervención, cuya ausencia convierte a la medida en desproporcionada. "Pues, de una parte, mal puede estimarse realizado ese juicio, en el momento de adopción de la medida, si no se manifiesta, al menos, que concurre efectivamente el presupuesto que la legitima. Y, de otra, sólo a través de esa expresión, podrá comprobarse ulteriormente la idoneidad y necesidad (en definitiva, la razonabilidad) de la medida limitativa del derecho fundamental (SSTC 37/1989, 3/1992, 12/1994, 13/1994, 52/1995, 128/1995, 181/1995 y 34/1996)" [STC 49/1999, F.Jº. 7º]. Estos presupuestos, fijados en el artículo 597.2 y 3 L.E.Crim. y coincidentes con la jurisprudencia del T.E.D.H. (reiterada en el caso Valenzuela

determinen la idoneidad, necesidad y proporcionalidad de la medida a adoptar[518]. Por último, todos estos presupuestos deben estar expresados en la referida decisión de intervenir la comunicación, de forma que se pueda acreditar que se han tenido en cuenta a la hora de adoptarla y, en su caso, de mantenerla. Es decir, que se pueda acreditar que se ha atendido a las circunstancias concretas del caso en cuestión[519].

Sobre la conexión entre la persona investigada y el hecho delictivo, se señala en el F.Jº. 8º, que ésta "se manifiesta en las sospechas, que como ha sostenido recientemente este Tribunal, no son tan sólo circunstancias meramente anímicas, sino que "precisan, para que puedan entenderse fundadas, hallarse apoyadas en datos objetivos, que han de serlo en un doble sentido. En primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control, y, en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o se va a cometer el delito sin que puedan consistir en valoraciones acerca de la persona" (STC 49/1999, F.Jº. 8º). Estas sospechas han de fundarse en "datos fácticos o indicios", en "buenas razones" o "fuertes presunciones" (SSTEDH caso Klass, caso Ludi, Sentencia de 15 de junio de 1992), o en los términos en los que se expresa el actual artículo 579 L.E.Crim. en "indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa" (artículo 579.1), o "indicios de responsabilidad criminal" (artículo 579.2).

Una vez verificados estos extremos, ya en el momento de llevar a cabo la intervención, de ejecutar la limitación del derecho al secreto de las

---

contra España, Sentencia del T.E.D.H. de 30 de julio de 1998, § 46 y ss.), residen en la existencia de una investigación en curso por un hecho constitutivo de infracción punible grave, en atención al bien jurídico protegido y a la relevancia social del mismo, y en la existencia de indicios sobre el hecho constitutivo de delito y sobre la conexión con el mismo de las personas investigadas".

[518] Ibídem (F.J. 3º) "En tercer lugar, afecta a la legitimidad de la decisión la falta de necesidad estricta de la medida; es decir, puede ser constitucionalmente ilegítima, dado su carácter prescindible, bien porque los conocimientos que pueden ser obtenidos carecen de relevancia respecto de la investigación del hecho delictivo o respecto de la conexión de las personas investigadas, o bien porque pudieran obtenerse a través de otras medidas menos gravosas de los derechos fundamentales en litigio" (SSTC 54/1996, F.Jº. 8º, 49/1999, F.Jº. 7º y 8º).

[519] Ibídem (F.Jº. 3º) "Por último, incide en la legitimidad de la medida la falta de expresión o exteriorización, tanto de la existencia de los presupuestos materiales de la intervención --investigación, delito grave, conexión de las personas con los hechos-- como de la necesidad y adecuación de la medida --razones y finalidad perseguida (STC 54/1996, F.Jº. 8º); y todo ello es exigible, asimismo, respecto de las decisiones de mantenimiento de la medida, en cuyo caso, además, deben ponderarse las concretas circunstancias concurrentes en cada momento y el conocimiento adquirido a través de la ejecución de la medida inicialmente prevista" (SSTC 181/1995, F.Jº. 6º, 49/1999, F.Jº. 11º).

comunicaciones por las autoridades competentes para ello, aprehendiendo el mensaje para poder acceder a su contenido, deben ser respetados y tomados en cuenta, dado que "puede resultar constitucionalmente ilegítima en la medida en que se verifique al margen de la cobertura judicial de la misma, es decir, excediéndose de los límites temporales --se mantiene la intervención más tiempo del habilitado--, personales --se investigan personas distintas de las autorizadas--, materiales --hechos diferentes--, u otros que constituyan condiciones judicialmente impuestas de la autorización (SSTC 85/1994, F.Jº. 3º, 86/1995, F.Jº. 3º, 49/1996, F.Jº. 3º, 121/1998, F.Jº. 5º)".

Y finalmente, respecto del control judicial[520] de la operación de intervención, señala el TC que en todo caso deben ser respetados los plazos en que se debe informar al Juzgado sobre los progresos e incidencias de la ejecución, así como de los resultados de la misma, ya que de otra forma se estaría incurriendo en una vulneración del derecho fundamental[521].

[520] Ibídem (F.Jº. 3º) "El control judicial puede resultar ausente o deficiente en caso de falta de fijación judicial de los períodos en los que debe darse cuenta al juez de los resultados de la restricción, así como en caso de su incumplimiento por la policía; igualmente, queda afectada la constitucionalidad de la medida si, por otras razones, el juez no efectúa un seguimiento de las vicisitudes del desarrollo y cese de la intervención telefónica, y si no conoce el resultado obtenido en la investigación (STC 49/1999, F.Jº. 5º)".

[521] Otras sentencias del Tribunal Constitucional relevantes respecto del necesario control judicial, son: STC 85/1994, de 14 de marzo (F.Jº. 3º); STC 181/1995, de 11 de diciembre (F.Jº.5º); STC 49/1996, de 26 de marzo (F.Jº. 3º); STC 54/1996, de 26 de marzo (F.Jº. 6º y F.J. 7º); STC 123/1997, de 1 de julio (F.Jº. 4º); STC 49/1999, de 5 de abril (F.Jº. 8º); STC 126/2000, de 16 de mayo (F.Jº. 6º); STC 14/2001, de 29 de enero (F.Jº. 2º) y, STC 202/2001, de 15 de octubre (F.Jº. 6º): "La necesidad de control judicial de la limitación del derecho fundamental exige aquí, cuando menos, que el Juez conozca los resultados de la intervención acordada para, a su vista, ratificar o alzar el medio de investigación utilizado [STC 49/1999, F.Jº. 11º y 171/1999, F.Jº 8º c) y 138/2001, F.Jº. 6º]. (F.Jº.7º): Debe aquí recordarse, en primer lugar, que hemos dicho (últimamente en las SSTC 121/1998, de 15 de junio, F.Jº. 5º; 166/1999, de 27 de septiembre, F.Jº. 2º; 236/1999, de 20 de diciembre, F.Jº. 4º, 122/2000, de 16 de mayo, F.Jº 3º; 126/2000, de 16 de mayo, F.Jº. 9º, y 14/2001, de 29 de enero, F.Jº. 4º) que no constituyen una vulneración del derecho al secreto de las comunicaciones las irregularidades cometidas en el control judicial a posteriori del resultado de las intervenciones telefónicas practicadas, pues dichas irregularidades no tienen lugar durante la ejecución del acto limitativo de derechos, sino en el momento de la incorporación de su resultado a las actuaciones sumariales. En definitiva, todo lo que respecta a la entrega y selección de las cintas grabadas, a la custodia de los originales y a la transcripción de su contenido no forma parte de las garantías derivadas del artículo 18.3 CE, sin perjuicio de su relevancia a efectos probatorios, pues es posible que la defectuosa incorporación a las actuaciones del resultado de una intervención telefónica legítimamente autorizada no reúna las garantías de control judicial y contradicción suficientes como para convertir la grabación de las escuchas en una prueba válida para desvirtuar la presunción de inocencia (SSTC 121/1998, F.Jº.5º 151/1998, F.Jº. 4º, y 49/1999, FF.JJº. 12º y 13º). Y, en segundo lugar, y en todo caso, ha de tenerse presente también que el control judicial puede resultar ausente o deficiente en caso de falta de fijación judicial de los períodos en los cuales debe darse cuenta al Juez de los resultados de la restricción, así como en caso de su incumplimiento por la policía. Igualmente ha de entenderse que queda afectada la constitucionalidad de la medida si, por otras razones, el Juez no efectúa un seguimiento de las vicisitudes del desarrollo y del cese de la intervención telefónica, y si no conoce el resultado obtenido en la investigación (SSTC 49/1999, F.Jº. 5º; 166/1999, F.Jº. 3º; 236/1999, F.Jº. 3º; 122/2000, F.Jº. 3º; y 299/2000, F.Jº. 7º)".

1.1.d.- Intervención del ordenador personal.

El contenido de un ordenador personal puede entenderse protegido por el derecho al secreto de las comunicaciones, a la intimidad y a la protección de datos personales, y sobre todo ello, en relación con la actuación de las autoridades policiales en un eventual registro, ha venido a poner luz la Sentencia de la Sala Segunda nº 173/2011 del Tribunal Constitucional, de 7 de noviembre, utilizando un concepto amplio de "privacidad", como esfera superior que abarca los ámbitos de la intimidad, el secreto de las comunicaciones y la protección de datos de carácter personal.

El fallo de esta resolución supone un importante cambio en la consideración jurisprudencial de la información conservada en dispositivos electrónicos de almacenamiento masivo de memoria, especialmente, los discos duros de los ordenadores, entendiendo que se trata de una importante fuente de información que permite conocer aspectos íntimos de la vida y personalidad del usuario. Y, aunque no exige el consentimiento expreso del usuario o propietario del dispositivo, si que exige tener en cuenta la "proporcionalidad" de la medida de intervención de un ordenador por las autoridades policiales sin necesidad de orden judicial: "si hay necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial" (F.Jº. 1º).

En el caso concreto, el Alto Tribunal entiende que el ordenador personal es un medio en el que se almacena "intimidad": "el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) – por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás

pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona*".*

Y además, respecto a la protección jurídica de las comunicaciones que puedan estar en él almacenadas, añade que: "el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del artículo 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (artículo 18.1 CE), en la medida en que estos correos o "email", escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información*"* (F.Jº. 2º).

Es interesante este párrafo, por cuanto se confirmar que el correo electrónico ya recibido, no está protegido por el "secreto comunicaciones"[522], sino por la "intimidad", y se detiene con precisión, en

[522] Del resumen publicado por el Profesor Lorenzo Cotino, Titular del Departamento de Derecho Constitucional de la Facultad de Derecho de la Universidad de Valencia, en su página personal:

explicar este concepto, dedicándole en el F.Jº. 2º un completo recorrido jurisprudencial y doctrinal, que interesa a la materia que nos ocupa.

Señala que la "intimidad", como derivación de la dignidad de la persona (artículo 10.1 CE): "implica la existencia de un 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"[523], concretando que el artículo 18.1 garantiza "un derecho al secreto, a ser desconocido, a que los demás no sepan que somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio" (SSTC 127/2003, de 30 de junio, F.Jº. 7º; 89/2006, de 27 de marzo, F.Jº. 5º).

Recuerda el Tribunal que 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 y la prohibición de hacer uso de lo así conocido[524]", y reconoce valor al consentimiento del individuo para acotar con precisión esa intimidad personal y familiar[525], pudiendo revocarlo en cualquier momento[526], ya haya sido prestado de forma tácita o expresa, verbalmente o "con actos concluyentes que expresen dicha voluntad" (STC 196/2004, de 15 de noviembre, F.Jº. 9º)[527]. Y, si estos límites son rebasados, considera también que se habrá quebrado la "conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida[528]".

---

http://www.cotino.net/2011/11/resumen-y-comentario-stc-7-11-2011-registro-policial-de-ordenador-sin-orden-judicial/

[523] SSTC 207/1996, de 16 de diciembre, F.Jº. 3º; 186/2000, de 10 de julio, F.Jº. 5º; 196/2004, de 15 de noviembre, F.Jº. 2º; 206/2007, de 24 de septiembre, F.Jº. 4º; 159/2009, de 29 de junio, F.Jº. 3º.

[524] SSTC 196/2004, de 15 de noviembre, F.Jº. 2º; 206/2007, de 24 de septiembre, F.Jº. 5º; 70/2009, de 23 de marzo, F.Jº. 2º.

[525] SSTC 83/2002, de 22 de abril, F.Jº. 5º; 196/2006, de 3 de julio, F.Jº. 5º.

[526] STC 159/2009, de 29 de junio, F.Jº. 3º.

[527] También llega a esta conclusión en las SSTC 22/1984, de 17 de febrero y, 209/2007, de 24 de septiembre respecto al derecho a la inviolabilidad del domicilio (18.2 CE), que el consentimiento no necesita ser "expreso" (F.Jº 3º de la primera) y que, "salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito" (F.Jº. 5º de la segunda).

[528] SSTC 196/2004, de 15 de noviembre, F.Jº. 2º; 206/2007, de 24 de septiembre, F.Jº. 5º; 70/2009, de 23 de marzo, F.Jº. 2º

Continúa el repaso insistiendo en que no estamos ante un derecho absoluto, pues no podrá "considerarse ilegítima aquella injerencia o intromisión en el derecho a la intimidad que encuentra su fundamento en la necesidad de preservar el ámbito de protección de otros derechos fundamentales u otros bienes jurídicos constitucionalmente protegidos (STC 159/2009 de 29 de junio, F.Jº. 3º)[529]", y concreta los requisitos que han de cumplirse para una inmisión justificada constitucionalmente en[530]:

- Principio de legalidad: "la existencia de un fin constitucionalmente legítimo; que la medida limitativa del derecho esté prevista en la ley*";*

- "Se acuerde mediante una resolución judicial motivada (si bien reconociendo que debido a la falta de reserva constitucional a favor del Juez, la Ley puede autorizar a la policía judicial para la práctica de inspecciones, reconocimientos e incluso de intervenciones corporales leves, siempre y cuando se respeten los principios de proporcionalidad y razonabilidad)";

- Principio de proporcionalidad: "si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)[531]*".*

El Tribunal Constitucional ha sido muy exigente a la hora de considerar acreditado si hay o no razones legítimas para permitir injerencias

[529] "A esto se refiere nuestra doctrina cuando alude al carácter no ilimitado o absoluto de los derechos fundamentales, de forma que el derecho a la intimidad personal, como cualquier otro derecho, puede verse sometido a restricciones (SSTC 98/2000, de 10 de abril, F.Jº. 5º; 156/2001, de 2 de julio, F.Jº. 4º; 70/2009, de 23 de marzo, F.Jº. 3º). Así, aunque el artículo 18.1 CE no prevé expresamente la posibilidad de un sacrificio legítimo del derecho a la intimidad -a diferencia de lo que ocurre en otros supuestos, como respecto de los derechos reconocidos en los arts. 18.2 y 3 CE-, su ámbito de protección puede ceder en aquellos casos en los que se constata la existencia de un interés constitucionalmente prevalente al interés de la persona en mantener la privacidad de determinada información".

[530] STC 70/2002, de 3 de abril, F.Jº. 10º, que resume la STC 207/1996, de 16 de diciembre, F.Jº. 4º.

[531] STC 89/2006, de 27 de marzo, F.Jº. 3º.

en el derecho a la intimidad, y considera en todo caso, que existirá esa justificación cuando se esté frente a un "interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal" (SSTC 25/2005, de 14 de febrero, F.Jº 6º; 206/2007, de 24 de septiembre, F.Jº. 6º)[532], coherentemente con los instrumentos jurídicos habilitados por el legislador para que las fuerzas y cuerpos de seguridad del Estado cumplan con esa función de averiguación del delito (artículo 282 LECrim, artículo 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado y, artículo 14 de la Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana)[533].

La Sentencia se detiene también en recordar la jurisprudencia recaída en materia de protección de datos [534], asumiendo la independencia de este derecho y, complementariedad para el derecho a la intimidad: "Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido,

[532] En efecto, "la persecución y castigo del delito constituye un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana, bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE" [SSTC 127/2000, de 16 de mayo, F.Jº. 3º a); 292/2000, de 30 de noviembre, F.Jº. 9º]. También "reviste relevancia e interés público la información sobre los resultados positivos o negativos que alcanzan en sus investigaciones las fuerzas y cuerpos de seguridad, especialmente si los delitos cometidos entrañan una cierta gravedad o han causado un impacto considerable en la opinión pública, extendiéndose aquella relevancia o interés a cuantos datos o hechos novedosos puedan ir descubriéndose por las más diversas vías, en el curso de las investigaciones dirigidas al esclarecimiento de su autoría, causas y circunstancias del hecho delictivo" (STC 14/2003, de 28 de enero, F.Jº. 11º).

[533] STC 70/2002, de 3 de abril, F.Jº 10º.

[534] (F.Jº.3º) "Así, hemos afirmado que "el derecho a la intimidad comprende la información relativa a la salud física y psíquica de las personas, quedando afectado en aquellos casos en los que sin consentimiento del paciente se accede a datos relativos a su salud o a informes relativos a la misma" (SSTC 70/2009, de 23 de marzo, F.Jº. 2º y 159/2009, de 29 de junio, F.Jº. 3º). También hemos dicho que "no hay dudas de que, en principio, los datos relativos a la situación económica de una persona entran dentro de la intimidad constitucionalmente protegida" (STC 233/1999, de 16 de diciembre, F.Jº. 7º), que "en las declaraciones del IRPF se ponen de manifiesto datos que pertenecen a la intimidad constitucionalmente tutelada de los sujetos pasivos" (STC 47/2001, de 15 de febrero, F.Jº. 8º), y que "la información concerniente al gasto en que incurre un obligado tributario, no sólo forma parte de dicho ámbito, sino que a través de su investigación o indagación puede penetrarse en la zona más estricta de la vida privada o, lo que es lo mismo, en los aspectos más básicos de la autodeterminación personal del individuo". (STC 233/2005, de 26 de septiembre, F.Jº. 4º). Por otra parte, en la STC 70/2002, de 3 de abril, en que un guardia civil había intervenido a un detenido una agenda personal y un documento que se encontraba en su interior, sostuvimos que "con independencia de la relevancia que ello pudiera tener a los fines de la investigación penal y, por tanto, de su posible justificación, debemos afirmar que la apertura de una agenda, su examen y la lectura de los papeles que se encontraban en su interior supone una intromisión en la esfera privada de la persona a la que tales efectos pertenecen, esto es, en el ámbito protegido por el derecho a la intimidad, tal como nuestra jurisprudencia lo define" (F.Jº. 10º). Finalmente, cabe recordar que en la STC 14/2003, de 28 de enero, F.Jº 6º, afirmamos que la reseña fotográfica de un detenido, obtenida durante su permanencia en dependencias policiales, "ha de configurarse como un dato de carácter personal", respecto del cual los miembros de las fuerzas y cuerpos de seguridad del Estado "están obligados en principio al deber de secreto profesional".

menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del artículo 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (artículo 18.1 CE), en la medida en que estos correos o "email", escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información" (F.Jº. 3º).

La Sala pone estas cuestiones doctrinales, o más bien conceptuales, en relación con la intervención policial de un ordenador

personal y los derechos fundamentales que podrían verse afectados, y se detiene a considerar la validez del consentimiento del usuario o propietario.

Según la Sentencia, es obvio que "el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno", pero matiza, que en aquellos supuestos que pueda verificarse la existencia de actos concluyentes de voluntad positiva, más allá de una simple falta de oposición a la intromisión domiciliaria, podrá entenderse que existe un consentimiento tácito, como por ejemplo, que el transmitente de una comunicación no active métodos de protección de la información permitiendo al destinatario e incluso a terceros (navegación o comunicaciones on-line abiertas) acceder a la información o datos de tráfico de la comunicación, sin restricciones.

En el caso de los ordenadores, y la potencial afectación de esferas íntimas de su propietario, el Tribunal Supremo recoge el principio de la proporcionalidad tanto para adoptar la medida de registro, como para ejecutarla (incautación y acceso), cuando es preciso hacerlo sin consentimiento del afectado[535], es decir, cuando concurran motivos justificados para una actuación policial inmediata. Señala que para ello, es preciso garantizar un mínimo control sobre la información a la que realmente se accede y, posteriormente, acreditar la necesidad, especialidad, y urgencia de la medida, así como la inmediata puesta en conocimiento o puesta a disposición de la autoridad judicial del objeto de la injerencia. El contenido de la memoria de un PC, es un elemento digno de protección y garantía jurídica, por el mero hecho de permitir desarrollar un "perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por

[535] Teniendo en cuenta el artículo 19 del Convenio europeo sobre la Cibercriminalidad, de 23 de Noviembre de 2001, el Anteproyecto de LO de desarrollo de los derechos fundamentales vinculados al proceso penal, que modificará la Ley de Enjuiciamiento Criminal, de Julio de 2011, recoge de forma prolija la regulación del registro de dispositivos electrónicos masivos, tanto a nivel de principios como de desarrollo procesal (arts. 347 y 348 del anteproyecto de la LECrim.). Asimismo, por ejemplo, el artículo 347.1 del anteproyecto, dice: "El examen, registro e incautación de los datos y archivos contenidos en ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos o sistemas de almacenamiento masivo de memoria, así como de los aparatos informáticos o de tecnología digital, sólo podrá realizarse con el consentimiento del titular o previa autorización del Juez de Garantías".

cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona"[536].

Es más, la Sentencia, se detiene en distinguir entre la información que se está comunicando o en proceso, y la que se almacena en el ordenador, negándole a ésta la protección que otorga el "derecho al secreto de las comunicaciones". Señala que la información que conserva en las memorias físicas o virtuales de los dispositivos de almacenamiento masivo de datos, está protegido por el derecho a la intimidad, siguiendo así lo ya apuntado por el Tribunal Constitucional en sus Sentencias 70/2002 y 123/2002, al reconocer que la protección del derecho al secreto de las comunicaciones, sólo alcanza al proceso de comunicación mismo, pero finalizado el proceso en que consiste la comunicación, la protección constitucional de lo recibido (incluido datos de tráfico o rastros de navegación) se realiza en su caos a través de las normas que tutelan la intimidad u otros derechos (todo ello como parte del concepto de "privacidad"), pues analizados en su conjunto, configuran un perfil preciso y descriptivo de su titular. Otra sentencia relevante en este sentido, es la STC 34/2009, sobre la acción de registrar el contenido de una agenda de un PC para conseguir direcciones de correo electrónico, y acceder al buzón de entrada de su cuenta de correo, y al contenido mensajes emitidos y recibidos por la denunciante perjudicada, en la que se focaliza la cuestión sobre las garantías del "derecho a la intimidad".

En general, se puede decir que el Tribunal Supremo establece un concepto amplio de "privacidad", para solventar la cuestión del registro de los ordenadores, y para ello se apoya también en jurisprudencia del Tribunal de Justicia de la Unión Europea que resume consideraciones esenciales[537] sobre el artículo 8 del Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales. Por ejemplo, en la Sentencia de 16 de febrero de 2000, dictada en el caso Amman contra Suiza, en el apartado 65 considera

[536] RODRÍGUEZ LAINZ, Jose Luis. Magistrado del Juzgado de Instrucción nº 4 de Córdoba. "Hacia un nuevo entendimiento de la protección integral de los dispositivos privados de almacenamiento electrónico de datos relativos a las comunicaciones (Comentario a la STC 173/2011, de 7 de Noviembre)". Revista ICAM *Otrosí*, nº 9. Enero – Marzo. 2012. Madrid. pp. 28 – 40.

[537] Véase también la Sentencia de 29 de enero de 2008, asunto C-275/06, Productores de Música de España (Promusicae) c. Telefónica de España SAU, apartados 61-70.

que el término "vida privada no se debe interpretar de forma restrictiva", pues "engloba el derecho del individuo de crear y desarrollar relaciones con sus semejantes", sin que "ninguna razón de principio permita excluir las actividades profesionales o comerciales". La Sentencia de 3 de abril de 2007, dictada en el caso Copland contra el Reino Unido, considera en su apartado 41 que están incluidos en el ámbito de protección del artículo 8 del Convenio Europeo *(por cuanto pueden contener datos sensibles que afecten a la intimidad)* tanto "los correos electrónicos enviados desde el lugar del trabajo" como "la información derivada del seguimiento del uso personal de Internet", y precisa en el apartado 42 que de no advertirse que podría ser objeto de un seguimiento, razonablemente cabe esperar que estemos ante información de carácter privado (correo electrónico y navegación por Internet). La Sentencia de 22 de mayo de 2008, dictada en el caso Iliya Stefanov contra Bulgaria, considera en su apartado 34 que "el registro de la oficina de un abogado, incluyendo los datos electrónicos, equivale a una injerencia en su "vida privada", lesiva por ello del artículo 8 del Convenio", y aunque en este caso, concurría un interés legítimo (investigación penal por delito de extorsión) y autorización judicial previa ("los registros del PC y las incautaciones deben, por regla general, deben llevarse a cabo en virtud de una orden judicial"), se había ejecutado por las autoridades de manera desproporcionada, afectado incluso al secreto profesional ("retiró todo el equipo del solicitante, incluyendo sus accesorios, así como todos los disquetes que se encontraban en su oficina, resultando que durante el tiempo que permaneció este material en su poder "ningún tipo de garantías existen para asegurar que durante el periodo intermedio el contenido completo del disco duro y los discos no fueron inspeccionados o copiados")[538].

[538] El Tribunal Constitucional, llega a conclusiones similares en la Sentencia 34/2009, de 9 de febrero, apreciando que no se había infringido por el órgano judicial "el principio de legalidad penal al haber condenado el demandante por un delito de descubrimiento y revelación de secretos, cuyo bien jurídico protegido es la intimidad, resultando como hechos probados que este había accedido al ordenador de una compañera de trabajo y había procedido a la lectura de sus mensajes de correo electrónico. En particular, reseñábamos que "Desde la estricta perspectiva de control que corresponde a este Tribunal en modo alguno cabe tildar a la vista del tipo penal previsto del artículo 197.1 y 2 CP de aplicación analógica o in malam parte, carente de razonabilidad por apartarse de su tenor literal o por utilización de pautas extravagantes o criterios no aceptados por la comunidad jurídica la llevada a cabo por la Audiencia Provincial, al considerar documentos personales e íntimos la libreta de direcciones y de teléfonos de la denunciante, accediendo por este medio a la dirección de su correo electrónico y subsumir en aquel tipo penal el acceso a dichos documentos sin el consentimiento de su titular, obteniendo de esta forma datos de carácter personal de aquella y de sus compañeros, que es la conducta por la que ha sido condenado el recurrente de amparo" (FJ6). A la misma conclusión hemos llegado respecto del acceso a los datos

Finalmente, se puede concluir que la Sentencia establece que, para determinados tipos de delitos, resulta crucial una intervención rápida del ordenador para asegurar la prueba (asegurar el tránsito de información sobre direcciones IP que se interconectan para compartir un archivo de contenido pedófilo), ante el riesgo de borrado o destrucción. Pero, en el caso concreto sobre el que se resuelve, aunque, la resolución explica que existía además un interés digno de reseñar: "la conveniencia de que por parte de los funcionarios policiales se comprobara con la conveniente premura la posibilidad de que existiesen otros participes, máxime en este caso en que se utilizó una aplicación informática que permite el intercambio de archivos, o que, incluso, detrás del material pedófilo descubierto, pudieran esconderse unos abusos a menores que habrían de acreditarse". (F.Jº. 4º), se emitió un Voto Particular que cuestionó si era tan urgente la intervención policial sin consentimiento del titular del dispositivo masivo de almacenamiento de datos, y si no podía haberse conservado la prueba de otro modo. En este sentido, la Magistrada Excma. Sra. doña Elisa Pérez Vera, explica que a su entender, el ordenador registrado estaba desconectado y precintado, y que la prueba estaba a salvo de cualquier tipo de manipulación[539].

almacenados en un teléfono móvil en la STC 230/2007, de 5 de noviembre, si bien declarando vulnerado en tal caso el artículo 18.3 CE "al haberse accedido por la Guardia Civil al registro de llamadas memorizado en el terminal intervenido al recurrente, confeccionando un listado de llamadas recibidas, enviadas y perdidas, sin su consentimiento ni autorización judicial (F.Jº. 2º)". (F.Jº. 4º).

[539] (…) "el acceso a archivos de Internet (como los que incriminaban al recurrente) sólo puede realizarse si el terminal en cuestión está conectado a la red, por lo que en nada se hubiera puesto en riesgo la labor investigadora de la Policía si, estando dicho terminal en su poder, se mantiene apagado hasta lograr la preceptiva autorización judicial. Por lo demás desde el día siguiente de la denuncia y de la entrega del ordenador el denunciado permaneció detenido en dependencias policiales, hasta que un día más tarde fue puesto a disposición judicial. De este modo durante veinticuatro de las cuarenta y ocho horas que tardó en dar cuenta al Juez de Instrucción, la Policía tuvo en dependencias policiales tanto el ordenador como al denunciado, cuyo comportamiento por tanto no podía poner en peligro ninguno de los elementos de prueba contenidos en aquél. (…) Estoy de acuerdo en que la entrada en el ordenador era una medida idónea e imprescindible para establecer todos los elementos del delito investigado. Pero no concurriendo la urgente necesidad de realizar esa intervención de manera inmediata, la misma debió llevarse a cabo con la autorización previa y el control de su ejecución por parte de la autoridad judicial, ya que durante el tiempo necesario para su obtención no existía riesgo de destrucción de las pruebas incriminatorias, ni se ponía en peligro la investigación policial. No habiéndose hecho así, tal actuación vulneró, en mi opinión, el derecho a la intimidad del actor, contaminando inexorablemente las pruebas obtenidas en la misma, sin que pueda considerarse sanada dicha vulneración por el conocimiento a posteriori por el Juez de Instrucción de la iniciativa policial, como parece apuntar la Sentencia, ni por el hecho de que a posteriori pudiera valorarse en sí misma como necesaria".

1.2.- Retención de datos:

1.2.a.- Antecedentes.

Es una realidad que las redes globales de comunicación son controladas por los usuarios y están sustituyendo gradualmente a la generación más antigua de redes nacionales de comunicaciones y, la persecución de los delitos debe también abarcar este nuevo ámbito de actuación. En este sentido, desde la Unión Europea se viene trabajando sólidamente en la implantación de medidas efectivas para la lucha contra los contenidos ilícitos en Internet, con el justo fin de proteger los derechos de los ciudadanos, promover el comercio electrónico y reforzar la seguridad en las transacciones.

En diciembre del año 1999, la Comisión Europea puso en marcha la iniciativa "e-Europa: Una sociedad de la información para todos"[540], con la intención de garantizar que Europa se beneficiase de las tecnologías digitales, y que la nueva sociedad de la información fuese socialmente "inclusiva". En junio del año 2000, el Consejo Europeo de Feira adoptó el "Plan de acción Europa", y solicitó que se aplicase antes de finales de 2002. Este plan de acción resaltaba la importancia de la seguridad de las redes y de la lucha contra la delincuencia informática, promoviendo medidas de actuación como el pionero Programa conocido como "Estudio COMCRIME", relativo a la delincuencia organizada, y que había sido adoptado por el Consejo de Justicia e Interior y aprobado por el Consejo Europeo de Amsterdam en el año 1997. Este programa invitaba a la Comisión Europea a realizar un estudio sobre la delincuencia informática. En el Consejo Europeo de Tampere[541] del año siguiente, se reconoció que los acuerdos promovidos

[540] Comunicación sobre una iniciativa de la Comisión para el Consejo Europeo extraordinario de Lisboa los días 23 y 24 de marzo de 2000. *E-europe: Una sociedad de la información para todos.* Disponible en: http://www.csae.map.es/csi/pdf/eeurope.pdf [22 de agosto 2009].

[541] El Consejo Europeo celebró una sesión especial en Tampere, los días 15 y 16 de octubre de 1999, sobre la creación de un espacio de libertad, seguridad y justicia en la Unión Europea. En las "Conclusiones de la Presidencia", se señalaba que el Consejo Europeo estaba resuelto a que la Unión se

en materia de definiciones y sanciones comunes de una serie de actos delictivos, debían también referirse a la delincuencia que utiliza las nuevas tecnologías, de forma que se facilitase la implantación de medidas útiles en el marco de la estrategia de la Unión, en materia de lucha contra la delincuencia que se sirve de las tecnologías.

La delincuencia informática se definió, en la Comunicación de la iniciativa "e-Europa: Una sociedad de la información para todos", en su sentido más amplio: "cualquier delito que de alguna manera implique el uso de tecnología de la información, y ello relación directa con el hecho de que para delinquir se beneficien de la disponibilidad de las redes de información y comunicación sin fronteras y de la circulación de datos, intangible y sumamente volátil". Asimismo recordaba que la delincuencia informática se comete en el ciberespacio, y que no se detiene en las fronteras nacionales geográficas, que puede perpetrarse desde cualquier lugar y contra cualquier usuario del mundo, y que requiere de una acción eficaz, tanto a nivel nacional como internacional.

Se ha reconocido ampliamente la necesidad de combatir la delincuencia informática y la necesidad de armonizar iniciativas al respecto, así por ejemplo, del conjunto de principios[542] y un plan de acción de diez puntos, aprobado por los Ministros de Justicia y de Interior en la Cumbre del G8, en Birmingham, en 1998, actualmente se están poniendo en práctica con la ayuda de un subgrupo especializado en delitos de alta tecnología, compuesto por representantes de las autoridades de control de los países de este Grupo, y siguiendo las directrices marcadas por la Comunicación de la Comisión, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, del año 2001, denominada: "Creación de una sociedad de la información más segura mediante la mejora de la seguridad

convirtiese en "un espacio de libertad, seguridad y justicia, utilizando plenamente las posibilidades que ofrece el Tratado de Ámsterdam". El Consejo Europeo lanzó un firme mensaje para confirmar la importancia de este objetivo, y acordó "una serie de orientaciones y prioridades políticas que convertirán rápidamente este espacio en una realidad".

[542] El Consejo de Justicia y Asuntos de Interior de la UE de 19 de marzo de 1998 aprobó los 10 principios para combatir la delincuencia de alta tecnología adoptados por el G8, e invitó a los Estados miembros de la UE no pertenecientes al G8 a unirse a la red.

de las infraestructuras de información y la lucha contra los delitos informáticos"[543].

Precisamente uno de los apartados más destacados y polémicos de esos diez puntos fue la conservación de los datos sobre tráfico, tanto histórico como futuro, por parte de los proveedores de servicio Internet a efectos de cumplimiento de las disposiciones legislativas y su puesta a disposición de las autoridades de control.

[543] La Comunicación define la delincuencia informática en un sentido amplio, como referido a todo delito que implique la utilización de las tecnologías informáticas. Los conceptos de "delincuencia informática", "delincuencia relacionada con la informática", "delincuencia de alta tecnología" y de "delincuencia cibernética", tienen el mismo significado en la medida que todos se refieren a: a) la explotación de las redes de información y comunicación sin ninguna dificultad geográfica y b) la circulación de datos intangibles y volátiles. Con el fin de mejorar la seguridad de las infraestructuras de la información, la Comisión estudia los distintos caminos que podría emprender con el fin de prevenir los delitos informáticos y de luchar contra ellos. Sobre la Retención de datos, señala que (5.2): "Para investigar y procesar delitos que implican el uso de las redes de comunicaciones, incluida Internet, las autoridades competentes utilizan frecuentemente los datos sobre tráfico cuando éstos son almacenados por los proveedores de servicios a efectos de la facturación. Como el precio de las comunicaciones depende cada vez menos de la distancia y del destino, los proveedores de servicios tienden a facturar tarifas planas, y ya no habrá necesidad de almacenar datos sobre tráfico para la facturación. Las autoridades competentes temen que esto suponga una reducción del material para investigaciones penales, y por tanto abogan por que los proveedores de servicios conserven algunos datos sobre tráfico por lo menos durante un período de tiempo mínimo, a fin de que puedan utilizarse a efectos de la aplicación de la ley. De conformidad con las Directivas de la UE sobre protección de datos personales, tanto los principios generales limitadores de la Directiva 95/46/CE como las disposiciones más específicas de la Directiva 97/66/CE, los datos sobre tráfico deberán destruirse o hacerse anónimos en cuanto termine el servicio de telecomunicación, a menos que sean necesarios a efectos de facturación. En los casos de tarifa plana o de acceso gratuito a los servicios de telecomunicaciones, no se permite en principio a los proveedores de servicios conservar los datos sobre tráfico. Conforme a las Directivas de la UE sobre protección de datos, los Estados miembros podrán adoptar medidas legales para limitar el alcance de la obligación de destruir los datos sobre tráfico, cuando dichas limitaciones constituyan una medida necesaria para, entre otros, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicaciones. No obstante, cualquier medida legislativa nacional que pueda prever la retención de datos sobre tráfico a efectos de la aplicación de la ley ha de cumplir determinados requisitos: las medidas propuestas deberán ser adecuadas, necesarias y proporcionadas, de acuerdo con el derecho comunitario y el derecho internacional, así como las Directivas 97/66/CE y 95/46/CE, el Convenio Europeo para la Protección de los Derechos Humanos de 4 de noviembre de 1950 y el Convenio del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales, de 28 de enero de 1981. (…). El Parlamento Europeo se ha expresado en el sentido de favorecer una obligación general de conservar datos sobre tráfico durante un período de tres meses" *(*Resolución legislativa que contiene el dictamen del Parlamento Europeo sobre el proyecto de Acción común, adoptada por el Consejo en virtud del artículo K.3 del Tratado de la Unión Europea, relativa a la lucha contra la pornografía infantil en Internet, enmienda 17 (DO C 219, 30.7.1999, pág. 68-71*).* "La Comisión considera que cualquier solución al complejo problema de la conservación de los datos sobre tráfico deberá tener un buen fundamento, ser proporcionada y lograr un equilibrio justo entre los distintos intereses en juego de las partes implicadas. (...) Existen intereses importantes y muy diversos que deben tenerse en cuenta. Por una parte, las autoridades de control de la protección de datos consideran que el medio más eficaz de reducir riesgos inaceptables para la intimidad, reconociendo al mismo tiempo la necesidad de aplicar eficazmente la ley, es que, en principio, los datos sobre tráfico no se conserven solamente a efectos de la aplicación de la ley. (…) "Es imprescindible prohibir la vigilancia exploratoria o general a gran escala... (…). El sector tiene interés en cooperar en la lucha contra delitos tales como la piratería y el fraude informático, pero no debería tener que hacer frente a medidas excesivamente costosas. (...) Habría que garantizar una seguridad adecuada de los datos sobre tráfico conservados". Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: "Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos" (COM (2000) 890 final - no publicada en el Diario Oficial). Disponible en: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_es.htm

A día de hoy, este aspecto concreto de la lucha contra la delincuencia informática sigue generando numerosos problemas a la hora de ser legislado y, de ser puesto en práctica.

El Grupo de Trabajo del Artículo 29 ya abordó estas cuestiones en la Recomendación 3/99[544], sobre la importante función que pueden ejercer los datos sobre tráfico en el contexto de la investigación de delitos cometidos a través de Internet, recordando a los poderes públicos nacionales, en la aplicación de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y de la Directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, el necesario respeto a los principios de protección de los derechos fundamentales y las libertades de las personas, y en particular que se deben tener en cuenta el derecho a la intimidad y al secreto de la correspondencia. Ambas Directivas se aplican al tratamiento de los datos personales en Internet, incluidos los datos sobre tráfico relacionados con abonados y usuarios[545].

Para la investigación y procesado de delitos que implican el uso de las redes de comunicaciones como Internet, son muy importantes los datos de tráfico almacenados por los proveedores de servicios a efectos de la facturación, pues permiten el rastreo de acciones hasta su autor. Sin embargo, estos rastreos, fuera del ámbito de las investigaciones de delitos y delincuentes, pueden conllevar graves injerencias en los derechos de los usuarios, especial y directamente en los derechos a la intimidad, a la protección de datos personales, y al secreto de las comunicaciones. La retención, tratamiento y conservación de los datos de conexión de las comunicaciones por parte de los operadores de telecomunicaciones y los proveedores de servicios de telecomunicación, ha de estar basado en el estricto cumplimiento de los fines que legalmente estén previstos tanto en

[544] Recomendación 3/99 del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada el 7 de septiembre de 1999.

[545] Los artículos 6, 7, 13 y los apartados 1 y 2 del artículo 17 de la Directiva 95/46/CE, y los artículos 4, 5, 6 y 14 de la Directiva 97/66/CE tratan específicamente la legitimidad de dicho tratamiento por los operadores de telecomunicaciones y proveedores de servicio.

el derecho comunitario como en el derecho interno de los Estados miembros de la Unión Europea. Cualquier medida legislativa nacional que pretenda prever la retención de datos sobre tráfico, ha de cumplir determinados requisitos y, en general, las medidas propuestas deberán ser adecuadas, necesarias y proporcionadas, de acuerdo con el derecho comunitario y el derecho internacional, así como las Directivas 97/66/CE y 95/46/CE, el Convenio Europeo para la Protección de los Derechos Humanos de 4 de noviembre de 1950 y el Convenio del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales, de 28 de enero de 1981.

Durante la Conferencia celebrada en Cardiff en los días 9 a 11 de septiembre de 2002, de Comisarios Europeos, esta cuestión fue tratada fue tratado, llegándose a la conclusión de que la finalidad principal de la retención de datos sobre tráfico de telecomunicaciones, debía ser el permitir el acceso a los organismos encargados de aplicar la ley y la seguridad, pero que en todo caso debía cumplir los requisitos básicos de legitimidad (proporcionalidad, necesidad y adecuación) y de confidencialidad[546]. Asimismo, se recomendaba el establecimiento de un plazo amplio de la conservación, que en un principio no debía ser superior a los tres meses, a fin de reducir al máximo los riesgos de acceso a la información por terceros no autorizados, aunque se amplió la propuesta hasta más de un año, y ello sin tener en cuenta los costes de implantación de medidas técnicas de seguridad que dichas medidas iban a requerir.

El Grupo de Trabajo del Articulo 29, en su Dictamen 5/2002, criticó duramente estos plazos. Teniendo en cuenta que, en ese momento, la protección de datos sobre tráfico de telecomunicaciones también estaba prevista por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas, y que en principio permitía el tratamiento de datos de tráfico para facturación y para pagos de interconexión y, en general, para la

[546] Grupo de Trabajo del Artículo 29. Dictamen 5/2002, sobre la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones. Doc. núm. 11818/02/ES/Final WP 64.

aplicación de la ley, estimó el Grupo de Trabajo que debía almacenarse esa información en todo caso "sólo por un período limitado y cuando constituya una medida necesaria proporcionada y apropiada en una sociedad democrática. Señaló expresamente que una retención sistemática de todas las clases de datos de tráfico para un período de un año o más sería claramente desproporcionada y, por lo tanto, inaceptable en todo caso".

En ese momento, cuando las Fuerzas y Cuerpos de seguridad requerían de los datos del titular de un teléfono móvil o de una dirección IP, para la investigación criminal que estuviesen siguiendo, contra delitos concretos, el proceso seguido exigía tan sólo que solicitaran a la autoridad judicial competente una orden que estableciese previamente las condiciones en que debía hacerse dicho requerimiento y que, en especial, controlase que efectivamente había motivos suficientemente fundados para restringir el derecho fundamental a la protección de datos personales de uno o más individuos. Con la nueva Directiva, se estableció un almacenamiento masivo de los datos de conexión, afectando tanto a quienes delinquen como a aquellos que no lo hacen.

Tres años más tarde, en el marco de las iniciativas europeas de lucha contra el terrorismo y la delincuencia organizada, y en el ambiente tenso propio de una Europa que acaba de ser golpeada por un nuevo ataque terrorista, esta vez en Londres (21 de septiembre de 2005), la Comisión Europea presentó una "Propuesta de Directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE" apremiando respuestas y, por ende, su aprobación.

El Grupo de Trabajo del Artículo 29, a través de su Dictamen 4/2005 sobre la propuesta de Directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modificaba la Directiva 2002/58/CE, adoptado el 21 de octubre de 2005, se volvió a pronunciar severamente sobre esta materia.

Entendía que el terrorismo estuviese planteando a nuestra sociedad "un desafío real y apremiante, pero señaló que los Gobiernos deben responder a este desafío de una manera que responda con eficacia a la necesidad de sus ciudadanos de vivir en paz y seguridad, sin socavar sus derechos humanos individuales, incluido el derecho a la confidencialidad de los datos, que constituyen una piedra angular de nuestra sociedad democrática. De hecho, la conservación de los datos del tráfico interfiere con el derecho fundamental e inviolable a la confidencialidad de las comunicaciones. Toda restricción a este derecho fundamental debe estar justificada por una necesidad apremiante, sólo deberá permitirse en casos excepcionales y deberá contar con las garantías adecuadas y por tanto, no es aceptable la imposición de dichas obligaciones de conservación de datos a los prestadores de servicios de comunicaciones sin establecer primero garantías adecuadas y específicas*".*

En una sociedad democrática, cualquier interferencia con este derecho fundamental podría justificarse sólo si es necesaria en interés de la seguridad nacional, pudiendo incluso llegar a vigilar y registrar todos los contactos y relaciones de los individuos, así como de los lugares donde tienen lugar y los medios utilizados para ello.

El Tribunal Europeo de Derechos Humanos también ha subrayado que la vigilancia secreta plantea el peligro de socavar o incluso destruir la democracia con el pretexto defenderla; además, ha afirmado que los Estados no pueden, en nombre de la lucha contra el espionaje y el terrorismo, adoptar cualesquiera medidas que consideren apropiadas[547]. Más aún, advierte que "los poderes de que disponen los cuerpos policiales en la lucha contra el terrorismo deberán ser eficaces, pero no pueden ser ilimitados ni utilizarse indebidamente. Debe alcanzarse un equilibrio proporcionado para garantizar que no se socave la sociedad que estamos intentando proteger. Este equilibrio es especialmente necesario cuando se trata de forzar a los prestadores de servicios de comunicaciones a que almacenen datos que ellos mismos no necesitan. De esta manera, podría

[547] Sentencia de 6 de septiembre de 1978, asunto Klass y otros contra Alemania. TEDH.

llegarse a un control continuo, generalizado y sin precedentes de todos los tipos de comunicación y movimiento de todos los ciudadanos en su vida diaria. Se almacenaría una enorme cantidad de información que sólo sería útil a efectos de investigación en un número limitado de casos"[548].

Sobre la propuesta de Directiva, también se pronunció en similares términos el Comité Económico y Social Europeo[549] a través de un Dictamen en el que comenzó manifestando "su extrañeza y preocupación por la presentación de una propuesta normativa de esta índole, pues su contenido resulta desproporcionado y afecta a los derechos fundamentales. Consideraba que el tratamiento dado en la propuesta a los derechos humanos, especialmente, el derecho a la intimidad, no se realiza adecuadamente y puede colisionar en determinados aspectos. Se corre el riesgo de socavar la confianza de los usuarios de las comunicaciones electrónicas y disminuir su disposición a utilizar las TIC. Esta pérdida de confianza por parte de los consumidores implica el riesgo de que el futuro desarrollo de la sociedad de la información se vea frenado a largo plazo (…)". Y específicamente, respecto del contenido de la propuesta, criticó con dureza el hecho de que incomprensiblemente, la Comisión "sólo toma en consideración los artículos 7 (respeto de la vida privada y familiar) y 8 (protección de datos de carácter personal) de la Carta, con olvido de otros preceptos, como son los artículos 36 (acceso a los servicios de interés general), 38 (protección de los consumidores), 47 (derecho a la tutela

[548] En esta materia, la opinión del Grupo de Trabajo del artículo 29 y de la Conferencia de las Autoridades Europeas de Protección de Datos desde 1997, ha sido firme y clara, cuestionando la necesidad de establecer medidas generales de conservación de datos y los límites que deben tenerse en cuenta. El Grupo de trabajo se ha pronunciado en este sentido en el Dictamen 9/2004 sobre un proyecto de Decisión marco (Documento del Consejo 8958/04, de 28 de abril de 2004), en cuyo anexo figura un resumen de las siguientes declaraciones: Dictamen 1/2003 sobre el almacenamiento de los datos sobre tráfico a efectos de facturación; Dictamen 5/2002 sobre la declaración de los Comisarios europeos de protección de datos en la Conferencia Internacional de Cardiff (9-11 de septiembre de 2002) sobre la conservación sistemática obligatoria de los datos de tráfico de las telecomunicaciones; Dictamen 10/2001 sobre la necesidad de un enfoque equilibrado en la lucha contra el terrorismo; Dictamen 4/2001 sobre el proyecto de convención del Consejo de Europa sobre la delincuencia cibernética; Dictamen 7/2000 sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, de 12 de julio de 2000; Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicios de Internet a efectos de cumplimiento de la legislación; Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones; Recomendación 3/97 sobre el anonimato en Internet.
Por su parte, la Conferencia Europea, se ha pronunciado expresamente en este sentido en las declaraciones adoptadas en Estocolmo (abril de 2000) y Cardiff (abril de 2002).

[549] Dictamen del Comité Económico y Social Europeo sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE. DOCE de 21 de Marzo de 2006.

judicial efectiva) o 48 (presunción de inocencia)". Este organismo reprende la actitud "descuidada" de la Comisión, y le invita a reflexionar *y* "actuar de forma más meticulosa y con escrupuloso respeto a los derechos fundamentales, para evitar en el futuro que los Tribunales Constitucionales de los Estados miembros declaren de inconstitucionales las normas que proponga", especialmente en lo que se refiera a que por defecto "la Comisión parece ignorar que, aunque los datos de su ámbito de aplicación son aparentemente "neutros" (identidad de los emisores y receptores de las comunicaciones, duración de éstas, localización física, frecuencia, etc.), se trata de elementos que invaden la vida privada de las personas y, en muchos casos, también pueden dañar otros derechos como el secreto profesional o la asistencia jurídica debida". Y ni siquiera se prevén normas que "impidan un eventual acceso de los proveedores y otros interesados a los datos almacenados, debiéndose prever que todo acceso a dichos datos deberán realizarse, solo en casos específicos y bajo control judicial".

Por último, destacar que el Comité recordó a la Comisión que debía tener en cuenta que "los particulares, sean o no ciudadanos de la Unión Europea, tienen el derecho a saber quién interfiere, por qué razones y con qué frecuencia sus comunicaciones, así como acceder a cualquier base de datos, pública o privada donde figuren este tipo de actuaciones"[550].

1.2.b.- La Directiva y su trasposición en España.

Teniendo en cuenta todas las recomendaciones antes dichas, en el ámbito de la UE fue aprobada la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público

[550] Sentencias del TEDH, de los asuntos Amann contra Suiza (2000), Kopp contra Suiza (1998), Halford contra Reino Unido (1997), y Malone contra el Reino Unido (1984).

o de redes públicas de comunicaciones[551], modificando la Directiva 2002/58/CE.

En el Considerando número 21 manifestaba que sus objetivos "son armonizar las obligaciones de los proveedores de conservar determinados datos y asegurar que éstos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la normativa nacional de cada Estado miembro, como el terrorismo y la delincuencia organizada, no pueden ser alcanzados de manera suficiente por los Estados miembros y, debido a la dimensión y los efectos de la presente Directiva, pueden lograrse mejor a nivel comunitario, la Comunidad puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado. Señala también en este mismo considerando que de conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos" y, especialmente para ello prevé un límite temporal máximo de 24 meses a la retención de los datos de tráfico de las comunicaciones[552].

También prevé un listado de categorías de datos que pueden ser almacenados por las operadoras o los proveedores de servicios de telecomunicaciones[553] y, las garantías que en todo caso deben ser respetadas para ello:

---

[551] "La lógica que se manifiesta en la Directiva sobre la conservación de los datos es la misma. Se afirma un poder absoluto del Estado de poner las manos sobre el "cuerpo electrónico" de los ciudadanos, frente al que se debe reaccionar reivindicando con fuerza un habeas data capaz de atribuir al cuerpo electrónico la protección que el habeas corpus, hace ochocientos años, dio al cuerpo físico, reaccionando a las pretensiones absolutistas del rey. La constitucionalización de la persona, visible al menos en el sistema de la Unión Europea, impone que nos movamos en esta dirección". RODOTÁ, S. "La conservación de los datos de tráfico en las comunicaciones electrónicas". En: Segundo Congreso sobre Internet, derecho y política: análisis y prospectiva (monográfico en línea). Revista de Internet, Derecho y Política. N.º 3. UOC. 2006. p. 56.
http://www.uoc.edu/idp/3/dt/esp/rodota.pdf

[552] Artículo 6 de la Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Períodos de conservación: 2Los Estados miembros garantizarán que las categorías de datos mencionadas en el artículo 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación".

[553] Artículo 5 de la Directiva 2006/24/CE. Categorías de datos que deben conservarse:
"1. Los Estados miembros garantizarán que las siguientes categorías de datos se conserven de conformidad con la presente Directiva:
a) datos necesarios para rastrear e identificar el origen de una comunicación: 1) con respecto a la telefonía de red fija y a la telefonía móvil: i) el número de teléfono de llamada, ii) el nombre y la dirección del abonado o usuario registrado; 2) con respecto al acceso a Internet, correo electrónico por

"Artículo 7. Protección y seguridad de los datos. Sin perjuicio de lo dispuesto en las disposiciones adoptadas de conformidad con las Directivas 95/46/CE y 2002/58/CE, los Estados miembros velarán por que los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones cumplan, en lo que respecta a los datos conservados de conformidad con la presente Directiva, como mínimo los siguientes principios de seguridad de los datos:

a) los datos conservados serán de la misma calidad y estarán sometidos a las mismas normas de seguridad y protección que los datos existentes en la red;

Internet y telefonía por Internet: i) la identificación de usuario asignada, ii) la identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía, iii) el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono;
b) datos necesarios para identificar el destino de una comunicación: 1) con respecto a la telefonía de red fija y a la telefonía móvil: i) el número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas, ii) los nombres y las direcciones de los abonados o usuarios registrados; 2) con respecto al correo electrónico por Internet y a la telefonía por Internet: i) la identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet, ii) los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación;
c) datos necesarios para identificar la fecha, hora y duración de una comunicación: 1) con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la comunicación, 2) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet: i) la fecha y hora de la conexión y desconexión del servicio de acceso a Internet, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, así como la identificación de usuario del abonado o del usuario registrado, ii) la fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario;
d) datos necesarios para identificar el tipo de comunicación: 1) con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado, 2) con respecto al correo electrónico por Internet y a la telefonía por Internet, el servicio de Internet utilizado;
e) datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación: 1) con respecto a la telefonía de red fija: los números de teléfono de origen y destino, 2) con respecto a la telefonía móvil: i) los números de teléfono de origen y destino, ii) la identidad internacional del abonado móvil (IMSI) y de la parte que efectúa la llamada, iii) la identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada, iv) la IMSI de la parte que recibe la llamada, v) la IMEI de la parte que recibe la llamada, vi) en el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio; 3) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet: i) el número de teléfono de origen en caso de acceso mediante marcado de números, ii) la línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación;
f) datos necesarios para identificar la localización del equipo de comunicación móvil: 1) la etiqueta de localización (identificador de celda) al comienzo de la comunicación, 2) los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.
2. De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación.

b) los datos estarán sujetos a las medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos;

c) los datos estarán sujetos a medidas técnicas y organizativas apropiadas para velar por que sólo puedan acceder a ellos las personas especialmente autorizadas, y

d) los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación".

Según STEFANO RODOTÁ, esta Directiva crea "naciones de sospechosos". Señala que "la multitud ya no es más "solitaria", como la describía en los años cincuenta el sociólogo americano David Riesman. Está ahora ya "desnuda", continuamente escrutada a través de las diversas tecnologías. Y la manera como está estructurada la Directiva manifiesta claramente que no nos enfrentamos a una situación transitoria: aquí el oxímoron "emergencia permanente" manifiesta toda su potencia y la regla "excepcional" se constituye como verdadera y estable disciplina del futuro"[554]

En España la norma que se aprobó para la efectiva transposición a nuestro ordenamiento jurídico de la Directiva 2006/24/CE, fue la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

En los trabajos preparatorios de esta norma, se publicó con fecha 21 de mayo de 2007, en el Boletín de las Cortes Generales nº 128, el Informe emitido por la Ponencia sobre el Proyecto de Ley de conservación de los datos relativos a las Comunicaciones Electrónicas y a las Redes

[554] RODOTÁ, S. "La conservación de los datos de tráfico en las comunicaciones electrónicas"… Op. Cit. p. 57.

Públicas de Comunicaciones. Resulta curioso que en este documento no se recogieran todas las enmiendas planteadas por los grupos parlamentarios, y que sin embargo, si fueron incluidas luego en la redacción final de la norma, como por ejemplo la que apuntaban Grupo Parlamentario de Izquierda Unida-Iniciativa per Catalunya Verds y el Grupo Parlamentario Vasco (EAJ-PNV), al entender que "resulta más adecuado a la jurisprudencia constitucional y europea de derechos humanos limitar la obligación de cesión únicamente en supuestos de delitos graves[555]. A este respecto, el Grupo Parlamentario Popular en el Congreso, planteaba en la enmienda nº 39, que si bien proponían que se limite la cesión de los datos retenidos a aquellos procesos penales que se sigan por delitos graves, se sugiere, sin embargo, para evitar los inconvenientes de la rigidez del sistema, una consideración de la gravedad del delito no coincidente con el criterio estrictamente cuantitativo que emplea el Código Penal (en su artículo 33.2)". Esto sin embargo no fue aceptado.

Otras enmiendas planteadas por los diputados, que destacan por su interés en la protección de los derechos fundamentales de los ciudadanos, fueron:

- La enmienda nº 2, del Grupo Parlamentario Vasco (EAJ-PNV), que proponía "adoptar el plazo mínimo establecido en la Directiva (6 meses), por su carácter menos restrictivo de los derechos fundamentales en juego". Coincide con esta limitación el Grupo Parlamentario Popular en el Congreso, en la enmienda nº 48, aunque alega motivos de eficiencia técnica. El plazo recogido en el texto definitivo de la Ley fue de 12 meses[556]. La enmienda nº 26, del Grupo Parlamentario de Izquierda Unida-Iniciativa per Catalunya Verds, en este sentido, fue aún más estricta, propuso sustituir "doce meses" por "noventa días", debido a que "el Convenio sobre Cibercriminalidad del Consejo

[555] Enmiendas nº 1 y nº 25. "Enmiendas e índice de enmiendas al articulado del Proyecto de Ley sobre Conservación de datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones". Boletín Oficial del Congreso de los Diputados, Nº 128 de 7 de mayo de 2007.
[556] Artículo 5.1 de la Ley 25/2007, de 18 de octubre. Período de conservación de los datos. "La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación".

de Europa propuso una duración máxima de conservación de los datos de 90 días, y fomentando la cooperación entre los Estados Miembros". El Grupo Parlamentario de Esquerra Republicana, en la enmienda nº 69, compartió la necesidad de un plazo de 90 días.

- La enmienda nº 5, del Grupo Parlamentario Catalán (Convergència i Unió), que proponía que, "en coherencia con lo dispuesto en el artículo 7 del Proyecto, que exige la "previa resolución judicial" como requisito de la cesión de los datos, debería insertarse esta expresión en el artículo 1, de modo que se elimine cualquier posibilidad de confusión al respecto, esto es, dejando claro cada vez que se menciona la cesión de los datos que la misma queda indisolublemente vinculada a la concesión previa de la autorización por la autoridad judicial competente".

- La enmienda nº 15, también del Grupo Parlamentario Catalán (Convergència i Unió), que critica que "las remisiones parciales del artículo proyectado podrían inducir al error de considerar que la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sea únicamente aplicable en los supuestos previstos en el mismo Proyecto, cuando la mencionada Ley Orgánica es aplicable a la totalidad del tratamiento y a la comunicación de los datos a los que se refiere el Proyecto, sin perjuicio de las previsiones específicas contenidas en el mismo". Esto finalmente no fue tomado en cuenta en la redacción final.

- La enmienda nº 28, del Grupo Parlamentario Popular en el Congreso, criticaba la redacción de un párrafo de la Exposición de Motivos, pidiendo la supresión de una parte del texto[557], por

[557] Se refiere al párrafo que, en la Exposición de Motivos, dice: "La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos. Y, el texto que fue finalmente suprimido, continuaba diciendo: un claro ejemplo lo constituye el uso de Internet como medio del que se sirven las

cuanto entendía que constituía "una afirmación que parece criminalizar Internet como si fuera una ciudad sin Ley, en la que los terroristas y delincuentes campan a sus anchas; cuando en realidad éste es un uso mínimo de una herramienta que ha supuesto una auténtica revolución y nos ha llevado a la Sociedad del Conocimiento. Un país como el nuestro, comprometido con el desarrollo de la Sociedad de la Información no debería hacer, en sus leyes, afirmaciones de este tenor".

- La enmienda nº 46 del Grupo Parlamentario Popular en el Congreso, que proponía añadir un segundo párrafo[558] al artículo 4.1 inicialmente proyectado, por el hecho de que este artículo no indicaba nada sobre la posibilidad que tienen lo prestadores de servicio de utilizar los listados de datos que ellos mismos recojan y conserven, creando "una laguna de regulación inadmisible en consideración a la confidencialidad de los datos que se manejan y a la afectación del derecho a la intimidad de los usuarios. Es preciso que la redacción del artículo, no sólo recoja la excepción al artículo 38[559] que ahora contiene, sino que vete una utilización propia hasta ahora no autorizada por la Ley".

Es preciso hacer una llamada de atención sobre el rango de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

El Grupo Parlamentario de Esquerra Republicana, en la enmienda nº 76, señaló la necesidad de cuestionar la aptitud de una ley ordinaria para

---

redes de delincuencia organizada, bandas terroristas o delincuentes individuales para contactar y comunicarse de manera barata, inmediata y camuflada entre el millonario número de comunicaciones que diariamente se efectúan a través de la red. Ante esta realidad, la sociedad demanda de las Autoridades que tienen encomendada la persecución de los delitos que se anticipen a la culminación de estas acciones criminales y proporcionen una respuesta eficaz, para lo cual deben contar con todos los medios técnicos, humanos y jurídicos necesarios".

[558] Se propuso añadir: "En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el propio artículo 38 de Ley General de Telecomunicaciones".

[559] Se refiere al artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, relativo a los Derechos de los consumidores y usuarios finales.

regular algunos de los aspectos que se estaban debatiendo y así, planteó una disposición final primera bis, con la siguiente redacción: "Naturaleza de la Ley. Las disposiciones contenidas en los artículos 1, 3, 4, 5, 6, 7 8 y 9 de esta Ley tienen el carácter de Orgánico. El resto de preceptos no tiene tal carácter". Las razones por las que planteaba esta precisión en la naturaleza de la norma, eran porque consideraba que "la conservación de datos del tráfico interfiere con el derecho fundamental e inviolable a la confidencialidad de las comunicaciones y a la protección de datos. El debate parlamentario de la Directiva 2006/24/CE que pretende transponer en el presente Proyecto de Ley ya manifestó posiciones discordantes con el objeto de la Directiva al entender que se podían vulnerar derechos fundamentales si no se establecían las suficientes garantías en el debate seguridad versus privacidad. Es, por ello, que consideramos que los artículos relativos al objeto de la Ley, en el que se excluye del ámbito de aplicación el contenido de las comunicaciones, el artículo 3, por el que se establecen los datos que deben ser objeto de conservación y el capítulo II (del artículo 4 al 9, inclusive) relativo a la conservación y cesión de datos deben ser objeto de mayor protección y su reforma debe requerir mayorías más calificadas, que las que requiere una Ley ordinaria".

La Ley fue aprobada como Ley Ordinaria, pero contenía una Disposición Final Primera que modificaba la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y la convertía en la base normativa de naturaleza orgánica de la interceptación de las comunicaciones y la conservación de los datos de tráfico por las operadoras, y matizando en todo caso que: "Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias".

1.2.c.- Reticencias en Europa.

El problema específico que directamente se trata de atajar con la retención y conservación de datos, es el uso anónimo de Internet, sin embargo, no todas las voces se muestran conformes con que este sea el medio más adecuado para lograrlo.

El Grupo de Trabajo del Artículo 29, desde hace más de una década, viene advirtiendo de la necesidad de que en cierta manera, se pueda mantener un uso anónimo de la Red.

En noviembre de 1997 una Recomendación específica a propósito del uso anónimo de Internet[560], en la que consideraba que la cuestión del anonimato es parte de un problema más complicado para Gobiernos y organizaciones internacionales, dado que el anonimato es de por si esencial para poder mantener libres de lesiones, en el ciberespacio, derechos fundamentales como la intimidad y libertad de expresión. Pero, por otra parte, el anonimato implica la oportunidad de observar y comunicarse en la red sin necesidad de revelar la identidad, lo que puede llevar la lucha a trabajar contra toda alteración del orden público, en el sentido de evitar la proliferación descontrolada de contenidos ilícitos y nocivos, el fraude financiero o las violaciones de los derechos de autor.

Señaló el Grupo de Trabajo del Artículo 29 que en el contexto de los más tradicionales medios de comunicación fuera de línea, tales como las cartas y paquetes, el teléfono, los periódicos, o la difusión por radio y televisión, se ha alcanzado un equilibrio entre la protección o garantía de los derechos fundamentales y, la restricción de éstos proporcionada a su ejercicio en circunstancias limitadas y concretas, y que esto debería mantenerse en el contexto del ciberespacio. Señaló asimismo que para que sea posible "este equilibrio, será vital el grado y los límites a la capacidad de participación en línea de forma anónima". Por otra parte, en la

[560] Recomendación 3/97 sobre el anonimato en Internet. Adoptada por el Grupo de Trabajo del artículo 29, el 3 de diciembre de 1997.

Declaración Final de la Conferencia Ministerial de Bonn sobre redes globales de información, celebrada los días 6-8 de julio de 1997, se estableció que, en los casos en que el usuario, en su actividad fuera de la red, pudiese elegir la opción de mantenerse anónimo, esta opción debería poder darse en el mismo sentido también en la red. Se entendió que "Internet no es un ghetto anárquico donde no se aplican las normas de la sociedad y que la capacidad de los Gobiernos y poderes públicos para restringir los derechos individuales y vigilar los comportamientos potencialmente ilícitos no debería ser mayor en las redes públicas que en el mundo exterior, fuera de la red".

Sin embargo, hoy esto es una utopía, pues las restricciones a los derechos y libertades fundamentales que en teoría deberían "ser adecuadamente justificadas, necesarias y proporcionadas a la vista de otros objetivos de orden público", están siendo tratadas con mucha mayor dureza en los ámbitos relativos a la telecomunicaciones, en aras de lograr una supuesta mayor protección contra el terrorismo y otras formas de delincuencia grave, pero lo cierto es que también, se está queriendo utilizar contra situaciones de naturaleza meramente económica que están perjudicando a determinados sectores industriales.

Y, reforzando estas consideraciones, el hito o consecuencia más importante se ha manifestado en Abril de 2011, de la mano de la Comisión Europea, que emitió un "Informe para el Consejo y el Parlamento Europeo, de evaluación sobre la Directiva de conservación de datos" (Directiva 2006/24/CE)[561].

Los datos de telecomunicaciones conservados por los operadores que son utilizados por la policía en la investigación, detección y enjuiciamiento de delitos graves y de terrorismo, son objeto de un tratamiento especial que ha de ser vigilado y regulado de forma que cumplan los especiales requisitos exigidos por el derecho comunitario. La Directiva sobre conservación de datos (Directiva 2006/24/CE) exige a los

[561] Informe de la Comisión al Consejo y al Parlamento Europeo. Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE). Disponible en: http://cde.gestiondocumental.info/juridica/aue/MAY11/30135.pdf

Estados miembros que garanticen que las operadoras de telefonía conserven determinadas categorías de datos personales[562] con fines de investigación, detección y enjuiciamiento de delitos graves tal como se definen en la legislación nacional, por un periodo de tiempo no inferior a seis meses ni superior a dos años (periodo que debe decidir cada Estado miembro al incorporar la Directiva a su legislación nacional).

Y tal y como se reconoce en la Comisión[563], mientras que las autoridades policiales y aduaneras de la mayoría de los Estados miembros insisten en lo esencial de la conservación de los datos, para la eficacia de las investigaciones criminales, las autoridades de protección de datos critican las medidas previstas por la Directiva, por cuanto no limita suficientemente la conservación de datos, ni ofrece garantías eficaces sobre la forma en que se tratan los datos[564].

En el Informe de la Comisión, se recuerda que la Directiva obliga a los Estados miembros a garantizar que los operadores respeten, como mínimo, cuatro principios de seguridad de los datos: "que los datos conservados sean de la misma calidad y estén sometidos a las mismas normas de seguridad y protección que los datos existentes en la red; que los datos estén sujetos a las medidas técnicas y organizativas adecuadas, para protegerlos de la destrucción accidental o ilícita, pérdida accidental o

[562] Aquellos datos personales útiles para identificar y proporcionar detalles sobre las llamadas telefónicas efectuadas y los correos electrónicos enviados, excluido el contenido de tales comunicaciones.

[563] "Nuestra evaluación demuestra la importancia que reviste el almacenamiento de datos de telecomunicaciones para los sistemas de justicia penal y para la aplicación de las leyes. Estos datos se utilizan como pruebas no sólo para condenar a los culpables de delitos graves o de terrorismo, sino también para eliminar las sospechas que puedan pesar sobre los inocentes. Por ejemplo, los datos conservados fueron fundamentales para el éxito de la Operación RESCUE, que ayudó a identificar a 670 personas sospechosas de pertenecer a una red internacional de pederastia y a proteger a los menores contra los abusos en los Estados miembros que han incorporado la Directiva. Ahora bien, el informe de evaluación también pone de manifiesto deficiencias importantes. Necesitamos un planteamiento común más proporcionado de este tema en toda la UE. Por ello tengo la intención de revisar la Directiva a fin de aclarar a qué personas se concederá acceso a los datos y para qué fines, así como los procedimientos que deberán seguirse". Cecilia Malmström, Comisaria de Asuntos de Interior. Disponible en: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/484&format=HTML&aged=1&language=ES&guiLanguage=en

[564] El Supervisor Europeo de Protección de Datos ha declarado que la Directiva "no ha logrado armonizar la legislación nacional" y que el uso de los datos conservados no se limita estrictamente a la lucha contra los delitos graves. Ha declarado que un instrumento de la UE que contenga normas sobre la conservación obligatoria de datos deberá, en caso de demostrarse su necesidad, contener también normas sobre el acceso de los servicios con funciones coercitivas y sobre su ulterior utilización. Ha invitado a la UE a que adopte un marco legislativo global que no sólo imponga a los operadores obligaciones de conservar datos, sino que también regule la manera en que los Estados miembros utilizan los datos a efectos de la aplicación de la Ley, al objeto de crear "seguridad jurídica para los ciudadanos". Discurso pronunciado por Peter Hustinx en la conferencia *Taking on the Data Retention Directive*, celebrada el 3 de Diciembre de 2010. Recogido en la página 35 del Informe de la Comisión.

alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos; que los datos estarán sujetos a medidas técnicas y organizativas apropiadas para velar por que sólo puedan acceder a ellos las personas especialmente autorizadas, y que los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación para los fines recogidos en la Directiva*".* Es decir, se busca garantizar que los datos retenidos no sean utilizados para otros fines no previstos, en consonancia con la Directiva de protección de datos y la Directiva sobre privacidad[565].

El Tribunal Constitucional rumano*[566]* (octubre de 2009), el Tribunal Constitucional Federal alemán*[567]* (marzo de 2010) y, el Tribunal Constitucional checo*[568]* (marzo de 2011) anularon sus respectivas leyes de transposición de la Directiva por considerarlas inconstitucionales[569]:

El Tribunal rumano aceptó que sólo se podía traspasar los límites de los derechos fundamentales en juego si se establecían salvaguardias adecuadas y suficientes para la protección contra posibles medidas arbitrarias del Estado, pero sobre la base de la jurisprudencia del Tribunal Europeo de Derechos Humanos[570], entendió que "la Ley de transposición era ambigua en su alcance y finalidad y que no contaba con suficientes salvaguardias, y alegó que "una obligación legal continuada" de conservar todos los datos de tráfico durante seis meses era incompatible con los derechos a la intimidad y la libertad de expresión del artículo 8 del Convenio Europeo de Derechos Humanos".

El Tribunal Constitucional alemán alegó que "la conservación de datos genera una percepción de control que podría obstaculizar el libre ejercicio de los derechos fundamentales", por lo que sólo se aceptaría la conservación de datos "para usos estrictamente limitados, junto con una

[565] Páginas 17 y 18 del Informe de la Comisión.
[566] Decisión nº 1258 del Tribunal Constitucional rumano de 8 de octubre de 2009.
[567] Bundesverfassungsgericht, 1 BvR 256/08, de 2 de marzo de 2010.
[568] Sentencia del Tribunal Constitucional de la República Checa de 22 de marzo sobre la Ley nº 127/2005 y Decreto nº 485/2005; véanse en particular los apartados 45-48, 50, 51 y 56.
[569] Páginas 23 y 24 del Informe de la Comisión.
[570] Tribunal Europeo de Derechos Humanos, Rotaru contra Rumania, 2000; Sunday Times contra Reino Unido, 1979; y Príncipe Hans-Adam de Liechtenstein contra Rumania, 2001.

seguridad de los datos suficientemente elevada", porque en si misma la "conservación de estos datos constituye una restricción grave del derecho a la intimidad y, por tanto, sólo debe ser admisible en circunstancias particularmente limitadas; y que un período de conservación de seis meses era el límite máximo ("an der obergrenze") que podría considerarse proporcionado (apartado 215)". Por otra parte, quiso precisar que los "datos sólo deberán solicitarse cuando ya exista una sospecha de delito grave o pruebas de peligro para la seguridad pública, y la obtención de datos debe prohibirse en determinadas comunicaciones privilegiadas (es decir, las relacionadas con necesidades sociales o emocionales) que se basan en la confidencialidad. Los datos también deberán codificarse con una supervisión transparente de su utilización".

El Tribunal Constitucional de la República Checa por su parte, estimó que la legislación de transposición no era suficientemente clara y precisa en su formulación, en concreto, no lo era la "definición de las autoridades competentes para acceder y utilizar los datos conservados, así como los procedimientos para dicho acceso y uso, no eran suficientemente claros en la legislación de transposición para garantizar la integridad y confidencialidad de los datos". No existían suficientes garantías contra posibles abusos de poder de las autoridades públicas.

Estos tres Estados miembros están estudiando cómo volver a transponer la Directiva[571].

En cuanto a las conclusiones de la Comisión, destacar cómo reconoce que debe velar "porque cualquier propuesta futura sobre conservación de datos respete el principio de proporcionalidad y sea adecuada para lograr el objetivo de la lucha contra el terrorismo y los delitos graves y no vaya más allá de lo que sea necesario para lograrlo".

[571] "También se han presentado asuntos de conservación de datos ante los tribunales constitucionales de Bulgaria, lo que dio lugar a una revisión de la Ley de transposición; de Chipre, donde se consideró que las resoluciones judiciales dictadas con arreglo a la ley de transposición eran anticonstitucionales; y de Hungría, donde está pendiente un asunto relativo a la omisión de los fines legales del tratamiento de datos en la legislación de transposición". Tribunal Supremo Administrativo búlgaro, Decisión n° 13627 de 11 de diciembre de 2008; Tribunal Supremo de Chipre, recurso nº 65/2009, 78/2009, 82/2009 y 15/2010-22/2010 de 1 de febrero de 2011; la solicitud de apreciación de la constitucionalidad fue presentada por la Unión de Libertades Civiles de Hungría el 2 de junio de 2008.

Asimismo, reconoce que las excepciones o limitaciones en lo que respecta a la protección de los datos personales sólo pueden aplicarse en la medida en que sean necesarias, "para la eficacia y eficiencia del sistema de justicia penal y para la aplicación de la ley, para la intimidad y para los costes de la administración pública y los operadores, de una regulación más estricta de la conservación, el acceso y el uso de los datos de tráfico".

Por último, cabe hacer referencia a las inquietudes que aún se pueden observar en el seno del Parlamento Europeo, respecto de las consecuencias prácticas de la transposición de la Directiva en los Estados miembros y, el proyecto de la nueva Directiva sobre retención de datos en que se trabaja. Así, con fecha 30 de mayo de 2011 el parlamentario Jan Philipp Albrecht, del Grupo de los Verdes/Alianza Libre Europea de Alemania (Verts/ALE), realizaba las siguientes preguntas al Parlamento:

- "¿Qué implicaciones extrajo la Comisión de la sentencia del Tribunal Constitucional alemán de 2 de marzo de 2010 sobre la conservación de los datos de las telecomunicaciones (1 BvR 256/08), teniendo en cuenta que dispone que, según la Directiva actual sobre la conservación de datos de telecomunicaciones (2006/24/CE(1)), prácticamente se había alcanzado el límite acumulativo absoluto de dichas medidas de conservación de datos y que, en consecuencia, el legislador está obligado a aplicar una limitación estricta en relación con las medidas adicionales de recopilación de datos de oficio (apartado 218)?"

- "¿Qué implicaciones extrajo la Comisión de dicha sentencia, teniendo en cuenta que determina un período de conservación de seis meses como límite superior aceptable en una sociedad democrática (apartado 215), en relación con el artículo 9 del proyecto de directiva, que introduciría un período de conservación de cinco años?"

La respuesta[572], poco precisa, la ofrecía la Comisaria europea de Interior, Cecilia Malmström, con fecha 23 de Junio de 2011, señalando que

[572] Disponible en: http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2011-005339&language=ES

el fallo del Tribunal Constitucional alemán "se refería al período correspondiente de retención de datos, conforme a las leyes de protección de datos, los datos no deben conservarse durante más tiempo del necesario. No hay un período de retención de datos único que se puede considerar que sea apropiado para todos los tipos diferentes de datos. El período de retención de datos adecuado para cada tipo diferente de base de datos debe ser juzgado por separado, es decir, por sus propios méritos".

1.3.- Interceptación de las comunicaciones:

1.3.a.- Cobertura legal.

La preocupación por las consecuencias de la interceptación de las comunicaciones en la vida de los ciudadanos europeos, fue plasmada en la Resolución del Consejo de la Unión Europea 96/C329/01, de 17 de enero de 1995, sobre la interceptación legal de las telecomunicaciones, y posteriormente, en la Resolución del Consejo, de 7 de Mayo de 1999, sobre la interceptación legal de las telecomunicaciones en relación con las nuevas tecnologías (sobre ENFOPOL, sistema europeo para la interceptación de las comunicaciones), y aunque no son vinculantes, vinieron a proporcionar una orientación armonizadora para los legisladores nacionales de los Estados miembros a la hora de abordar el desarrollo de previsiones legales en este cometido.

En España, es el artículo 55 de la CE[573] el que recoge las garantías que es necesario observar en una situación extraordinaria de interceptación

[573] Artículo 55 CE:
"1. Los derechos reconocidos en los artículos 17, 18, apartados 2 y 3; artículos 19, 20, apartados 1, a y d, y 5, artículos 21, 28, apartado 2, y artículo 37, apartado 2, podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución. Se exceptúa de lo establecido anteriormente el apartado 3 del artículo 17 para el supuesto de declaración de estado de excepción".

policial de las comunicaciones, antes de proceder a suspender el derecho al secreto de las comunicaciones, y prevé que si no se dan las condiciones precisas "la utilización injustificada o abusiva de las facultades reconocidas en dicha Ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las Leyes". Es decir, que sólo una Ley Orgánica podrá determinar la forma y los casos en los que se podrá proceder a ello, en relación con personas determinadas y, respecto a investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. Por tanto, las únicas interceptaciones posibles son las previstas por el artículo 579 de la Ley de Enjuiciamiento Criminal[574] y, por la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. Y en este contexto, la Ley General de Telecomunicaciones[575] en su artículo 33, concreta las condiciones en que deberá plantearse su ejecución por los operadores que prestan los servicios de telecomunicaciones accesibles al público.

Es claro que el derecho interno español permite límites o restricciones al derecho fundamental de secreto de las comunicaciones,

---

2. Una Ley Orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas.
La utilización injustificada o abusiva de las facultades reconocidas en dicha Ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las Leyes".

[574] Artículo 579 de la L.E.C., en la redacción según Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal:
"1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.
2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.
3. De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.
4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación".

[575] Artículo 33 LGT. Secreto de las comunicaciones.
"Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias. Asimismo, los operadores deberán adoptar a su costa las medidas que se establezcan reglamentariamente para la ejecución de las interceptaciones dispuestas conforme a lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia".

aunque habrán de venir ordenadas por una resolución judicial, al menos en principio, y deberán estar fundadas en alguna de las siguientes causas[576]:

> - "La finalidad de descubrir o comprobar hechos relevantes para la causa penal.
>
> - La existencia de indicios de responsabilidad criminal en la persona afectada por la interceptación o que se sirva de las comunicaciones para la realización de sus fines delictivos.
>
> - La necesidad de la medida de cumplimiento de las funciones asignadas al Centro Nacional de Inteligencia".

La última norma aprobada en esta materia, en desarrollo de estas pautas, es el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril. Supuestamente su articulado contiene previsiones de ejecución material de la interceptación de las comunicaciones, y ha sido muy criticado por no observar las debidas garantías constitucionales, especialmente la de que todo límite sea previsto por una norma con rango de Ley Orgánica o, que su ejecución esté fundada en todo caso en una orden judicial.

A partir del año 2001, en España se empezó a trabajar en las tareas de implementación de un software de interceptación de las comunicaciones, almacenamiento y reutilización de la información obtenida. Se trataba del Sistema Integral de Interceptación de las Comunicaciones Electrónicas: SITEL, propiedad del Ministerio del Interior. De su gestión se encarga la Dirección General de Infraestructuras (depende de la Secretaria de Estado para la Seguridad del Estado) y, está instalado en los

[576] Informe del Ministerio de Justicia sobre el proyecto de Real decreto por el que se establecen los procedimientos y las medidas técnicas para la interceptación legal de las telecomunicaciones, exigibles a los operadores de servicios de telecomunicaciones disponibles al público y de redes públicas de telecomunicaciones, de fecha 29 de Abril de 2003, remitido al Ministerio de Ciencia y Tecnología, como parte de los trámites preceptivos, previsto por el artículo 24.2 de la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración Pública.

proveedores de servicios de redes de telecomunicación (ISP) y centralizado en los "Centros de Interceptación".

Este sistema debe ser puesto en relación directa con otro similar denominado OSEMINTI (Infraestructura de Inteligencia Semántica Operacional), en el que también participaban Francia e Italia, y que permitía que los servicios de Inteligencia, por medio de ordenadores, identificasen frases (voz/texto) con determinado significado, e incluso aprendiesen de ello, de forma que se convertía en uno de los sistemas de espionaje más avanzados en comprensión de mensajes.

Respecto del aval jurídico de SITEL, la norma que desarrolla su funcionamiento, el contenido y ejecución de la interceptación legal de las comunicaciones, es el Real Decreto 424/2005, de 15 de Abril, aprobado por el Consejo de Ministros, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios[577], Reglamento cuyo Título V contiene un Capítulo II que regula expresamente "La interceptación legal de las comunicaciones" (artículos 83 a 101), y que ha sido duramente criticado por los motivos que se exponen a continuación.

El funcionamiento de SITEL, de los Centros de Interceptación de las comunicaciones y la entrega de la información a través de la Red SITEL, ha sido muy criticado.

Básicamente[578] se trata de conservar el contenido de las comunicaciones y los datos de tráfico en un servidor anónimo situado en un centro de interceptación, donde son consultados a través por un agente "facultado".

Posteriormente, de la información obtenida, se realizan grabaciones autenticadas de la misma, para ser aportadas a la autoridad judicial que

[577] Publicado en el Boletín Oficial del Estado número 102, de fecha 29 de Abril de 2005.
[578] Informe elaborado por la Comisaría General de policía Judicial del Cuerpo Nacional de Policía, sobre el sistema operativo SITEL, a solicitud de la Audiencia Provincial de Madrid, Sección 1, en oficio libre con nº de Identificación único 7015609/2009, Rollo: 31/2009, en fecha 4 de Enero de 2011.

ordenó la interceptación (en soportes no reescribibles, no repudiables), garantizando su contenido mediante una aplicación de firma electrónica avanzada y reconocida. Los grupos operativos encargados de la investigación, no acceden en ningún momento al sistema central de almacenamiento, sino que realizan volcados de la información en dichos soportes.

El problema es que si el juez ordena que se retiren ciertas partes de las conversaciones, por su carácter privado y ajeno, estas son eliminadas a los solos efectos de su presentación al procedimiento judicial (del CD que finalmente se incorporaría a la causa), pero no de la base de datos que inicialmente almacenó las conversaciones interceptadas. El contenido integro de la comunicación quedará en el servidor "sine die", con independencia de lo que pase después, ya sea archivado el procedimiento, ya se ordene no continuar por ser irrelevante el contenido de la interceptación, o ya sea absuelto el afectado.

A esto se añade, que el control judicial que se prevé para la operación, aparentemente no es demasiado efectivo, pues se permite la observación de los datos de tráfico de las comunicaciones por los "agentes facultados", para cualquier "investigación legal"[579], incluso aunque el juez no lo incluya en la orden de interceptación.

Por otra parte, parece también que estas operaciones no cuentan siquiera con la cobertura legal necesaria para poder ser utilizadas como medio de investigación y prueba valida en un proceso, tal y como exige la jurisprudencia del TEDH, del Tribunal Constitucional y del Tribunal Supremo[580]. En los trabajos preparatorios del polémico Proyecto de Real Decreto que regula SITEL, se contó con los preceptivos informes de los Ministerios y entidades públicas afectadas (tales como el Consejo General

[579] Artículo 89 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

[580] Informe dictaminado en Junio de 2006, como conclusión de unas diligencias de investigación, por el Teniente Fiscal de Madrid, Pedro Martínez. Informe que elevó al Fiscal General del Estado, Cándido Conde Pumpido Touron, en el que se indicaba que SITEL había sido utilizado sin cobertura jurídica alguna, y que el Reglamento aprobado un año mas tarde de su puesta en marcha era insuficiente, pues la Constitución exigía que se regulase mediante Ley Orgánica.

del Poder Judicial o la Agencia Española de Protección de Datos) y, aunque las conclusiones se mostraron en general favorables a la aprobación de la norma, lo cierto es que se mostraron ciertos matices y alguna particularidad en relación con las personas autorizadas para realizar las interceptaciones. Así por ejemplo, el Ministerio del Interior[581] puso de relieve al legislador que la definición de "Agente Facultado" no era todo lo precisa que cabría esperar y, que debía se modificada por cuanto "únicamente pueden existir dos categorías de agentes facultados: la Policía Judicial y los miembros del Centro Nacional de Inteligencia, y estos últimos no tienen la consideración de agentes de la autoridad, ni de Policía Judicial" (…). Por otra parte, recuerda que sólo la Policía Judicial, en ejercicio de sus funciones de investigación del delito[582], "puede y debe acceder a la información previa, mediando un requerimiento justificado", requerimiento que debe entenderse hecho a los operadores, sobre datos de conexión que tengan retenidos y, hecho por la autoridad judicial competente o a petición de la Policía Judicial en el marco de una investigación penal.

Por su parte, el Ministerio de Defensa, estimó en su Informe de fecha 21 de febrero de 2001, que "no resulta absolutamente claro que el Proyecto de Real Decreto informado se limite a desarrollar el artículo 49 de la Ley General de Telecomunicaciones (actual artículo 33), puesto que no regula las obligaciones de los operadores para garantizar el secreto de las telecomunicaciones, sino a sensu contrario, sus obligaciones a la hora de interceptar legalmente las mismas. De la obligación de garantizar el secreto de las telecomunicaciones no se desprende la obligación de interceptarlas. En esta duda sobre el rango de la norma proyectada redunda el hecho de estar regulando el ejercicio de limitaciones a un derecho fundamental".

El Informe de la Agencia Española de Protección de Datos, de fecha 27 de septiembre de 2002, califica la ejecución de las interceptaciones

[581] Informe emitido por la Secretaría General Técnica del Ministerio del Interior, al Proyecto de Real Decreto por el que se establecen los procedimientos y las medidas técnicas para la interceptación legal de las comunicaciones electrónicas exigibles a los operadores que presten servicios o exploten redes de comunicaciones electrónicas disponibles al público, de fecha 8 de Julio de 2003.

[582] Artículos 104 y 126 de la Constitución, artículo 11 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, artículo 445 de la Ley Orgánica del Poder Judicial, artículo 228 de la Ley de Enjuiciamiento Criminal, artículo 2 del Real decreto 769/1987, de 19 de junio, de regulación de la policía judicial y, artíclo22 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

como "cesiones de datos de carácter personal que se verifican sin el previo consentimiento del interesado" y, por tanto, que se deben ajustar a lo dispuesto por el artículo 11.2 de la Ley Orgánica 15/1999 de protección de datos de carácter personal, que exige que dichas cesiones estén previstas en una Ley. En el caso que nos ocupa, debe tenerse en cuenta que esta normativa excluye de su ámbito de aplicación los ficheros de carácter personal sometidos a la normativa sobre protección de materias clasificadas, así como a los ficheros establecidos para la investigación del terrorismo y, de formas graves de delincuencia organizada y, que además, se trata de la articulación de unas cesiones de datos inconsentidas habilitadas por normas con rango de Ley, sin embargo, nada obsta para que se realicen con el máximo rigor y respeto al artículo 18 de la CE.

El que podría calificarse como el más completo de los Informes emitidos, en relación con este Proyecto de Real Decreto, y lo que se refiere a la calidad de la norma para regular dichos contenidos y la capacidad de los órganos competentes para llevar a cabo las interceptaciones, es tal vez el Informe del Consejo General del Poder Judicial, de fecha 24 de octubre de 2002. En este informe consideró que debía expresar su parecer sobre aquello que afectase directamente a derechos y libertades fundamentales y así, señaló expresamente que:

> "Efectivamente, el artículo 18.3 de la Constitución Española consagra como derecho fundamental el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, "salvo resolución judicial".
>
> Por su parte, el artículo 55.2 de la CE dispone que una Ley Orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en el artículo 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas".

Reconocía la necesidad de que mediase una resolución judicial motivada, fundamentada "en la finalidad de descubrir o comprobar hechos relevantes para la causa penal, en la existencia de indicios de responsabilidad criminal en la persona afectada por la interceptación o que se sirva de las comunicaciones para la realización de sus fines delictivos" y, reconoció además la necesidad de que quienes ordenen la interceptación esté claramente definidos como "autoridad judicial" por la norma: "Se evitaría así confusión en cuanto a la posibilidad de que otra autoridad u organismo distinto de una autoridad judicial pueda confirmar o autorizar la adopción de una medida de interceptación de las comunicaciones, en caso de que la adopción haya sido ordenada por alguna de las autoridades gubernativas a que hace referencia el artículo 579.4 de la Ley de Enjuiciamiento Criminal o por el Secretario de Estado Director del Centro Nacional de Inteligencia, en el supuesto previsto en la Ley Orgánica 2/2002*".*

Por último, y desde el punto de vista de los afectados, de los usuarios de las comunicaciones electrónicas interceptadas, destaca la preocupación por la definición de autoridad judicial y "autoridad competente", como aquellas figuras facultadas para autorizar la adopción y ordenar la ejecución técnica de una medida de interceptación legal y, para materializar la interceptación, respectivamente.

El Informe emitido por la Asociación Española de Proveedores de Servicios de Internet (AEPSI), en septiembre de 2002, al borrador del Proyecto del Real Decreto, recordaba en este sentido que "los jueces o tribunales son los únicos que tienen capacidad legal para autorizar y ordenar dicha interceptación y siempre previa existencia y comunicación al sujeto obligado de la orden judicial correspondiente. Además, sería conveniente que este Real Decreto definiese, a fin de agilizar y clarificar la actuación del sujeto obligado, las especificaciones que deberá incorporar la orden judicial de interceptación. Entre ellas debería figurar específicamente el sujeto o sujetos obligados a realizar la interceptación (para clarificar responsabilidades individuales y duplicidad en la actuación), la información específica relativa a la interceptación requerida (puesto que ésta dependerá

del tipo de comunicación), el centro de recepción de la interceptación y otros datos que faciliten el proceso de interceptación. Con la introducción de todas estas especificaciones en la orden judicial, dicha actuación se beneficiaría también de una mayor proporcionalidad".

La AEPSI, consideró que esto debía ser así por coherencia con la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, que en su artículo 12 establece las obligaciones en materia de retención de datos y, que únicamente faculta a los jueces y tribunales o, al Ministerio Fiscal, como autoridades competentes para requerir los datos de tráfico relativos a las comunicaciones electrónicas[583].

En definitiva, todos los informes parecen coincidir en la necesidad de que sea un juez quien ordene y controle la interceptación de las comunicaciones, pero, sin entrar en el detalle de los aspectos que pueden quedar al margen de ello, aceptan que:

> "La información previa a la interceptación legal no forma parte del contenido intelectual de los mensajes transmitidos, conforme explica la Fiscalía General del Estado en la consulta 1/1999, de 22 de enero, acerca del tratamiento de datos personales en el ámbito de las telecomunicaciones. En consecuencia, los contratos entre operadores y clientes, los DNI de los abonados, los pasaportes o tarjetas de residencia, domicilio y números y características de los terminales de los usuarios, no están integrados en el derecho fundamental al secreto de las comunicaciones"[584].

Finalmente, el resultado normativo de estos debates se traduce en que, con fecha 29 de abril de 2005, fue publicado en el Boletín Oficial del Estado nº 102, el Real Decreto 424/2005, de 15 de abril, por el que se

[583] Este Informe va más allá, y señala a continuación que "En caso de que se decidiese habilitar para la materialización de la interceptación a otra "autoridad competente" al margen de la judicial, debería definirse explícitamente en el BRDILT".
[584] Informe emitido por la Secretaría General Técnica del Ministerio del Interior, de fecha 8 de julio de 2003.

aprobaba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. El Capítulo II, en el Título V, regula "La interceptación legal de las comunicaciones" (artículos 83 a 101).

Dos años después, con fecha 19 de octubre de 2007, fue publicada en el Boletín Oficial del Estado nº 251, como "complemento" del anterior, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, por cuanto su Disposición Final Primera vino a dar nueva redacción al artículo 33 de la Ley 33/2003, de 3 de noviembre, General de Telecomunicaciones, para proporcionar la cobertura legal necesaria a los preceptos del Real Decreto 424/2005, de 15 de abril.

1.3.b.- Respaldo de los tribunales.

La primera de esas dos normas fue llevada a los tribunales por la Asociación de Internautas[585], siendo desestimadas sus pretensiones por entenderlas carentes de objeto a raíz de la publicación de la segunda, cosa que se produjo mientras el proceso seguía pendiente. Poco después, en el año 2008, tras solicitar al Defensor del Pueblo[586] que planteara el oportuno Recurso de Inconstitucionalidad ante el Tribunal Constitucional frente a la Ley 25/2007, de 18 de octubre y, serle denegado con fecha 18 de enero de 2008, por entender que el rango legal ordinario era suficiente para regular determinadas garantías constitucionales del artículo 18 de la CE, para

[585] Con fecha 29 de junio de 2005, fue interpuesto en nombre de la Asociación de Internautas, ante el Tribunal Supremo, el oportuno Recurso Contencioso – Administrativo frente al Real Decreto 424/2005, de 15 de abril, por cuanto se consideraba que una norma de carácter reglamentario no podía regular la restricción de derechos fundamentales, tales como el secreto de las comunicaciones o la protección de datos, porque se opondría a la Constitución Española.

[586] Escrito de fecha 9 de enero de 2008, presentado ante el Defensor del Pueblo, a fin de que plantease el oportuno Recurso de Inconstitucionalidad, contra la Ley 25/2007, de 18 de Octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, por vulneración de los artículos 18, 55 y 81 de la Constitución Española y, en general, por prescindir de las garantías esenciales que otorga la reserva de ley orgánica y, el control judicial en la restricción de derechos fundamentales.

regular en concreto la inexistencia de control judicial previo en la interceptación de las comunicaciones, la Asociación de Internautas decidió enviar su denuncia ante la Comisión Europea.

El objeto de la impugnación ante Europa se centraba no sólo en la inadecuación del rango legal de esta norma para contener las limitaciones de un derecho fundamental, según lo dispuesto por el artículo 55 de la CE, sino también en el contenido[587] del apartado 8 del artículo 33 de la Ley

[587] Artículo 33 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Secreto de las comunicaciones.
1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.
2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de Ley Orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.
3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.
4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.
El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.
5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante Real Decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:
- Identidad o identidades del sujeto objeto de la medida de la interceptación. - Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.
- Identidad o identidades de las otras partes involucradas en la comunicación electrónica. - Servicios básicos utilizados. - Servicios suplementarios utilizados. - Dirección de la comunicación. - Indicación de respuesta. - Causa de finalización. - Marcas temporales. - Información de localización. - Información intercambiada a través del canal de control o señalización.
6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante Real Decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:
- Identificación de la persona física o jurídica. - Domicilio en el que el proveedor realiza las notificaciones. Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:
- Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado). - Número de identificación del terminal. - Número de cuenta asignada por el proveedor de servicios Internet. - Dirección de correo electrónico.
7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso

32/2003, de 3 de noviembre (LGT), por ser el que se refiere específicamente a actuaciones previas a la ejecución de la interceptación, en concreto a cesiones de datos de carácter personal inconsentidas.

Es decir, denunciaba esta Asociación que una norma de rango legal no orgánico, estaba previendo una cesión de datos de carácter personal no consentidas por sus titulares, sin previa autorización judicial; que se preveía una limitación de derechos fundamentales en una norma de rango inferior y sin el control judicial que exige el propio artículo 33 de la Ley General de Telecomunicaciones en su apartado tercero: "Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas*".*

A este respecto el Defensor del Pueblo[588], el Tribunal Supremo[589] y, el Consejo General del Poder Judicial[590] emitieron sendas respuestas, en la

---

de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.
8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.
9. Los sujetos obligados deberán tener en todo momento preparada una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.
10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.
Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.

[588] Resolución del Defensor del Pueblo de fecha 18 de Enero de 2008.

[589] Sentencia del Tribunal Supremo, Sala de lo Contencioso Administrativo, Sección tercera, de fecha 5 de Febrero de 2008.

[590] Informe emitido por el Consejo General del Poder Judicial, al Proyecto de Real Decreto por el que se establecen los procedimientos y las medidas técnicas para la interceptación legal de las comunicaciones electrónicas exigibles a los operadores que presten servicios o exploten redes de comunicaciones electrónicas disponibles al público, de fecha 24 de octubre de 2003.

instancia de la denuncia correspondiente, y sin embargo lo hicieron en igual sentido, conviniendo que los de carácter personal a que se refiere dicho precepto, son accesorios[591], no son parte del derecho al secreto de las comunicaciones y, por tanto, pueden tratarse al margen del contenido de la orden judicial que acuerda la interceptación.

Justifica su postura el Consejo General del Poder Judicial en su Informe diciendo que:

> "Dentro de los específicos supuestos legales de interceptación de las comunicaciones y, con carácter previo a que ésta se lleve a cabo, se establece en el artículo 7 el deber de los sujetos obligados a facilitar a la autoridad competente información relativa a los identificadores de punto de terminación de red, de terminal, los códigos de identificación, servicios y características del sistema de telecomunicación que utilizan los sujetos sometidos a la medida de interceptación y, si disponen de ellos, los nombres de los abonados con sus números de DNI, tarjeta de residencia o pasaporte, si se trata de personas físicas, o bien denominación y CIF, si se trata de personas jurídicas.
>
> Este deber de suministrar información previa, que no menoscaba el secreto de las comunicaciones, así como la obligación que se impone a los sujetos obligados de tener dispuesta la organización necesaria – de personas y procedimientos – para garantizar el cumplimiento de una orden de interceptación, se estima muy positivo en orden a dotar de las máximas garantías de seguridad a una medida que, en cuanto supone una excepción o suspensión temporal

[591] "Y la ausente conservación de los contenidos de las comunicaciones corre el peligro de volverse un boomerang, no una garantía. Si he hecho una llamada telefónica inocente a quien luego se revela un criminal, la imposibilidad de demostrar cuál ha sido el verdadero contenido de la comunicación dejará sobre mí la sombra de la sospecha. Una sospecha que incluso puede ser construida: visto que deben registrarse también los intentos de llamada no conseguidos, alguien podría llamarme en un momento en el que sabe que no me encuentro en condiciones de contestar, creando así la apariencia de una relación que me une a esa persona, que yo podría incluso no conocer". RODOTÁ, S. "La conservación de los datos de tráfico en las comunicaciones electrónicas"… Op. Cit. p. 58.

de un derecho constitucional, ha de tener un carácter restrictivo en su aplicación y especialmente garantista en su ejecución".

La misma línea interpretativa siguieron los informes de los otros dos organismos.

Esta teoría fue rebatida con ocasión de la Sentencia de fecha 5 de Febrero de 2008, por la que finalmente el Tribunal Supremo desestimaba las pretensiones de la Asociación de Internautas, ya que el Magistrado del Tribunal Supremo D. Óscar González González la contradijo severamente en un interesante Voto Particular. Comienza su razonamiento diciendo que:

"Discrepo con todo respeto del parecer de la opinión mayoritaria, y entiendo que debió plantearse al Tribunal Constitucional cuestión de Inconstitucionalidad de los apartados 6º y 7º del artículo 33 de la Ley 32/2003, de 3 de Noviembre, General de Telecomunicaciones, en su redacción de la Ley 25/2007, de 18 de Octubre, como previa al dictado de la sentencia y, en caso de que se estimara por aquel la inconstitucionalidad de dichas normas, habría que dictar sentencia anulando el real Decreto inicialmente impugnado, en lo concordante con dichos preceptos".

Señala además que la "autorización al agente facultado para obtener datos no incluidos en el mandamiento judicial no puede ampararse en el artículo 579 de la Ley de Enjuiciamiento Criminal (ley orgánica), pues en él sólo se regula la resolución judicial de interceptación, sin que se autorice a la policía ir más allá de su contenido. Tampoco puede apoyarse en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial del Centro Nacional de Inteligencia, cuyo artículo único, somete a la autorización judicial la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones llegando incluso a limitar el contenido de la solicitud, pero en cualquier caso, siempre dentro del contenido de la orden judicial".

Sobre la intervención previa de "agentes facultados" en la interceptación de las comunicaciones, señaló el Tribunal Supremo en su Sentencia que corresponde en todo caso "a las autoridades judiciales competentes, resolver acerca de la legitimidad de la obtención de los datos a los que se haya tenido acceso con carácter previo a la orden legal de interceptación" (F.Jº.7º). Ante esta afirmación en la que reconoce expresamente que la intervención judicial en estas situaciones lo es a posteriori, se pregunta el Magistrado discrepante:

> "(...) los apartados 6º y 7º del artículo 33, en los que se impone a los sujetos obligados a facilitar al agente facultado una serie de información, que puede no estar incluida en la orden de interceptación". (...) "Por muy interesante que estos datos puedan resultar para la investigación policial, no puede dejar de reconocerse que son muy personales, y rebasan con mucho la mera instrumentalidad. La propia sentencia implícitamente viene a reconocerlo, cuando indica que la autoridad judicial podrá excluirlos de la orden de interceptación, lo que implica que son algo más que un simple instrumento sin el cual la orden no puede cumplirse. Por otra parte, si la Ley impone al agente facultado el deber de pedir los datos del apartado 6 y 7 del artículo 33, no se entiende como puede el órgano judicial disponer, en contra de la norma, que los referidos datos no se emitan. Se trata de datos esenciales que no tienen por qué ser conocidos por terceras personas, salvo que así lo disponga la orden de interceptación (...)."

Es decir, comparte el Magistrado, con la Asociación denunciante, el hecho de que una norma de rango legal no orgánico, está previendo la cesión de datos de carácter personal no consentidas por sus titulares, con carácter previo a la adopción de la preceptiva autorización judicial, es decir, una limitación a derechos fundamentales en una norma de rango inferior y sin control judicial.

La opinión del Tribunal Constitucional, sobre estas cuestiones, también es importante. En un primer momento, se podría decir que el Alto Tribunal no consideraba relevante, a efectos constitucionales, el hecho de que una norma de rango inferior a la Ley Orgánica regule posibles limitaciones a un derecho fundamental, o que se produzcan cesiones de datos sin el amparo legal que prevé la Constitución, pues sin entrar en el fondo de la cuestión, así lo expresó en la Providencia, de la Sección Segunda de la Sala Primera, de fecha 10 de febrero de 2009, en respuesta al Recurso de Amparo promovido por la Asociación de Internautas, contra la Sentencia de fecha 5 de febrero de 2008 antes mencionada: "el recurrente no ha satisfecho la carga consistente en justificar la especial trascendencia constitucional del recurso (artículo 49 de la Ley Orgánica del Tribunal Constitucional, redactado por la Ley Orgánica 6/2007, de 24 de mayo), que es algo más y distinto a la mera afirmación – sobre cuya verosimilitud nada cabe decir- de que el propio derecho fundamental ha sido violado".

Sin embargo, si tenemos en cuenta que los motivos de la impugnación no eran tanto la vulneración del derecho, sino la trascendencia constitucional del hecho de que se mantenga en vigor una norma legal contraria a la Constitución, y cómo esto afecta directamente a derechos fundamentales, se pone de manifiesto una doctrina constitucional ciertamente cercana a los argumentos del Magistrado D. Óscar González González, que se muestra a continuación.

En cuanto a la necesaria tutela de una Ley Orgánica para materias a ella reservadas, la STC 142/1999, señalaba la necesidad de que fuese una Ley Orgánica la que regulase las restricciones de derechos fundamentales[592] y, la STC 127/1994 se refería a esto en idéntico sentido, en relación con el concepto de "desarrollo de derechos fundamentales y libertades públicas".

[592] (F.J.16º) - (…) "cabe considerar que la regulación de determinados aspectos, esenciales para la definición del derecho, la previsión de su ámbito y la fijación de sus límites en relación con otras libertades constitucionalmente protegidas, son elementos necesarios del «desarrollo» normativo a realizar por Ley Orgánica. Pero, aparte de estos elementos esenciales y necesarios, la Ley Orgánica puede ampliar el contenido del derecho de que se trate, o bien puede remitir a leyes ordinarias la regulación de aspectos que no resulten decisivos o capitales en su configuración (…) En el presente caso, es claro que la representación ante administraciones públicas de organizaciones o asociaciones no es el elemento definidor o necesario del derecho de asociación; y que, en los términos en que ha de interpretarse el artículo 9.1 de la Ley (según señalamos en el F.Jº. 13º) no supone una restricción de ese derecho" (…).

Señalaba el Tribunal Constitucional que es necesaria una Ley Orgánica cuando se incide directamente sobre ese ámbito y límites, como el caso que nos ocupa[593].

Por otra parte, la STC 292/2000, que es si cabe la más relevante en materia del derecho a la protección de datos y su posible restricción por normas de carácter reglamentario en cumplimiento de un mandato legal[594], se refiere la necesidad de que las cesiones de datos inconsentidas sean en todo caso autorizadas por normas de rango legal. Y esto ha de ponerse en relación con el artículo 53.1 de la CE y, por extensión directa, con el artículo 55.2 de la CE, que exige que la ley que determine la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas, sea Ley Orgánica. Además, en esta Sentencia se reconoce el importante papel de los poderes públicos para hacer efectiva la garantía de los derechos fundamentales[595], en este caso, sobre los datos de carácter personal que pueden considerase protegidos y el papel de los poderes públicos en su protección / restricción, entiende que[596]:

---

[593] (F.Jº. 3º) - "De este modo, hemos reconocido que "la función de garantía adicional" que cumple el artículo 18.1 de la Constitución en materia de derechos fundamentales "conduce a reducir su aplicación a las normas que establezcan las restricciones de esos derechos y libertades" o los "desarrolle" de modo directo "en cuanto regulen aspectos consustanciales con los mismos, excluyendo, por tanto, aquellas otras que simplemente afecten a elementos no necesarios sin incidir directamente sobre su ámbito y límites" [STC 101/1991, F.Jº.2º, que invoca las SSTC 160/1987, 161/1987 (RTC 1987/161), 57/1989 (RTC1989) y 132/1989 (RTC 1989/132)]".

[594] (F.Jº.2º) – (…) "la cesión de datos inconsentida autorizada por una norma infralegal, soslaya que el artículo 53.1 CE reserva en exclusiva a la Ley la regulación y limitación del ejercicio de un derecho fundamental, vulnerando por consiguiente el derecho fundamental mismo, al privarle de una de sus más firmes garantías".

[595] (F.J. 6º) – "Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin". (F.Jº .10º)- "De este modo, la LOPD puede ser contraria a la Constitución por vulnerar el derecho fundamental a la protección de datos (artículo 18.4 CE), por haber regulado el ejercicio del haz de facultades que componen el contenido del derecho fundamental a la protección de datos de carácter personal prescindiendo de las precisiones y garantías mínimas exigibles a una Ley sometida al insoslayable respeto al contenido esencial del derecho fundamental cuyo ejercicio regula (artículo 53.1 CE)".

[596] Se transcriben literalmente una selección de los párrafos que se consideran más relevantes de los numerosos y extensos fundamentos jurídicos de la STC 202/2000.

(F.Jº. 9º) – "el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal".

Es decir, ha de entenderse que el artículo 18.4 de la CE protege también aquellos datos personales que siendo públicos, accesibles al conocimiento de cualquiera, "identifiquen o permitan la identificación del individuo, (...) pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo", porque datos personales no sólo los datos relativos a la "vida privada o íntima de la persona". Y por eso, cualquier tratamiento que de ellos se haga vulnerando las normas que lo regulan, sobre su contenido o sobre las facultades decisorias que implica para el individuo, supondrá la imposición de límites constitucionalmente ilegítimos. La Ley debe prever los límites de los derechos fundamentales, evitando hacerlos impracticables, y respetando su contenido esencial. No se puede habilitar a un poder público "para fijar en cada caso las restricciones que pueden imponerse" (...) "incluso si la Ley habilitante enumera con detalle los bienes o intereses invocables por los Poderes Públicos en cuestión, o que sus decisiones sean revisables jurisdiccionalmente (que lo son en cualquier caso, con arreglo al artículo 106 CE)". La ley así elaborada infringirá el mandato constitucional de la reserva de Ley "frustrando así una de las garantías capitales de los derechos fundamentales en el Estado democrático y social de Derecho (artículo 1.1 CE)" (F.Jº. 11º)[597]. El desarrollo reglamentario de una Ley es un complemento a ésta, y no puede implicar "una renuncia del legislador a su facultad para establecer los límites a los derechos fundamentales, transfiriendo esta facultad al titular

[597] SSTC 83/1984, de 24 de julio [RTC 1984, 83], F.jº. 4º., 137/1986, de 6 de noviembre [RTC 1986, 137] , F.Jº. 3º, 254/1994, de 21 de septiembre [RTC 1994, 254] , F.Jº. 5º.

de la potestad reglamentaria, sin fijar ni siquiera cuáles son los objetivos que la reglamentación ha de perseguir, pues, en tal caso, el legislador no haría sino deferir a la normación del Gobierno el objeto mismo reservado"[598] (F.Jº. 14º). La STC 83/1984, explicaba en este mismo sentido que las remisiones legales a la potestad reglamentaria, deben hacerse a un complemento sin el que la Ley no se pueda aplicar.

Por tanto, sólo el legislador estará legitimado constitucionalmente para "determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias", en virtud de la reserva de Ley del artículo 53.1 CE. (F.Jº. 16º).

Por lo que se refiere al segundo aspecto destacado de la regulación vigente analizada, a la necesidad de una autorización judicial previa a la interceptación de las comunicaciones, se puede citar la STC 188/1999, que se pronuncia específicamente sobre la necesidad de que las medidas restrictivas de derechos fundamentales sean comunicadas a las autoridades judiciales a fin de que puedan proceder al control de su ejecución y, determinar los aspectos más sensibles de la misma[599]. La STC 104/2006, siguiendo la misma línea señala que la autorización judicial es necesaria precisamente para determinar, a priori lógicamente, "los elementos necesarios para ponderar que la medida se ajusta al principio de proporcionalidad y que se ha acordado, no como medida prospectiva genérica para la investigación delictiva, sino en relación con personas y hechos delictivos determinados, respecto de concretas líneas telefónicas con

[598] STC 227/1993, de 9 de julio [RTC 1993, 227], F.Jº. 4º, recogiendo la expresión de la STC 77/1985, de 27 de junio [RTC 1985, 77] , F.Jº. 14º.

[599] (F.Jº 8º) – "Así lo ha entendido este Tribunal Constitucional, en numerosas Sentencias dictadas a este respecto, cuando ha dicho que las "resoluciones administrativas de intervención de las comunicaciones, no sólo han de cumplir lo dispuesto en los arts. 18.3 y 25.2 C.E. y en el artículo 51 L.O.G.P., especialmente la motivación prevista en el artículo 51.5 L.O.G.P., sino, en cuanto medida que supone el sacrificio de un derecho fundamental, también han de cumplir el presupuesto de que se persiga con ella un fin constitucionalmente legítimo y los requisitos de que la medida sea adoptada mediante resolución de la Dirección del Centro especialmente motivada, que la misma sea notificada al interesado y que sea comunicada al Juez para que éste pueda ejercer el control sobre ella" (SSTC207/1996, 128/1997 y 175/1997).

sujeción a plazos prefijados"[600] y, la STC 253/2007, viene a confirmar lo anteriormente expuesto, señalando la importancia de que sean observados los requisitos de la resolución judicial que ordena la interceptación de una comunicación y las garantías constitucionales, en aras de la proporcionalidad y de la mínima intervención que exige toda acción penal[601].

A mayor abundamiento, es interesante conocer también que el Tribunal Constitucional se ha basado en la doctrina jurisprudencial del Tribunal Europeo de Derechos Humano para fundamentar algunas de sus resoluciones sobre injerencias en el derecho a la intimidad y vida privada (artículo 8 CEDH) en relación con medidas de interceptación de comunicaciones y la ausencia de previsión legal de dicha injerencia. Por ejemplo, la STC 184/2003 cita en su F.Jº. 4º diversas resoluciones europeas habidas en esta materia: Sentencias de 2 de agosto de 1984, caso Malone c. Reino Unido (párrafos 66 y ss., y 79); de 24 de abril de 1990, casos Kruslin

[600] (F.Jº 2º) - "(…) ciertamente, la adecuación a la Constitución de la restricción del derecho al secreto de las comunicaciones (artículo 18.3 CE) precisa, entre otras condiciones, haberse autorizado judicialmente en resolución en la que deben exteriorizarse, por sí misma o mediante su remisión a la solicitud de la autoridad que solicita la intervención, los elementos necesarios para ponderar que la medida se ajusta al principio de proporcionalidad y que se ha acordado, no como medida prospectiva genérica para la investigación delictiva, sino en relación con personas y hechos delictivos determinados, respecto de concretas líneas telefónicas con sujeción a plazos prefijados. De forma que las resoluciones judiciales de autorización de las intervenciones telefónicas deben contener datos relativos al marco espacial —líneas telefónicas delimitadas—, temporal —plazos—, objetivo —hechos delictivos investigados— y subjetivo —personas conectadas con los hechos delictivos y titulares o usuarios de las líneas telefónicas— de la misma, y la ejecución policial de la medida debe efectuarse en el marco fijado en las autorizaciones judiciales (por todas, STC 171/1999, de 27 de septiembre, F.Jº. 7º)".

[601] (Continúa el F.Jº 2º) - "En este sentido tenemos dicho que la resolución judicial en la que se acuerda la medida de intervención telefónica o su prórroga debe expresar o exteriorizar las razones fácticas y jurídicas que apoyan la necesidad de la intervención, esto es, cuáles son los indicios que existen acerca de la presunta comisión de un hecho delictivo grave por una determinada persona, así como determinar con precisión el número o números de teléfono y personas cuyas conversaciones han de ser intervenidas, que, en principio, deberán serlo las personas sobre las que recaigan los indicios referidos, el tiempo de duración de la intervención, quiénes han de llevarla a cabo y cómo, y los períodos en los que deba darse cuenta al Juez para controlar su ejecución (SSTC 49/1996, de 26 de marzo, F.Jº. 3º; 236/1999, de 20 de diciembre, F.Jº. 3º; 14/2001, de 29 de enero, F.Jº. 5º). Así pues, también se deben exteriorizar en la resolución judicial, entre otras circunstancias, los datos o hechos objetivos que puedan considerarse indicios de la existencia del delito y la conexión de la persona o personas investigadas con el mismo, indicios que son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento. Esto es, sospechas fundadas en alguna clase de dato objetivo (SSTC 171/1999, de 27 de septiembre, F.Jº. 8º; 299/2000, de 11 de diciembre, F.Jº. 4º; 14/2001, de 29 de enero, F.Jº. 5º; 138/2001, de 18 de junio, F.Jº. 3º; y 202/2001, de 15 de octubre, F.Jº. 4º). Tales precisiones son indispensables, habida cuenta que el juicio sobre la legitimidad constitucional de la medida exige verificar si la decisión judicial apreció razonadamente la conexión entre el sujeto o sujetos que iban a verse afectados por la medida y el delito investigado (existencia del presupuesto habilitante), para analizar después si el Juez tuvo en cuenta tanto la gravedad de la intromisión como su idoneidad o imprescindibilidad para asegurar la defensa del interés público, pues la conexión entre la causa justificativa de la limitación pretendida –la averiguación del delito– y el sujeto afectado por ésta –aquél de quien se presume que pueda resultar autor o participe del delito investigado o pueda haberse relacionado con él– es un prius lógico del juicio de proporcionalidad". (SSTC 49/1999, de 5 de abril, F.Jº. 8º; 166/1999, de 27 de septiembre, F.Jº. 8º; 171/1999, de 27 de septiembre, F.Jº. 8º; 126/2000, de 16 de mayo, F.Jº. 7º; 299/2000, de 11 de diciembre, F.Jº. 4º; 14/2001, de 29 de enero, F.Jº. 5º; 138/2001, de 18 de junio, F.Jº. 3º; 202/2001, de 15 de octubre, F.Jº. 4º).

c. Francia (párrafos 34 y ss.), y Huvig c. Francia, (párrafos 34 y ss.); de 23 de noviembre 1993, caso A. c. Francia, (párrafo 38 y ss.); de 25 de marzo de 1998, caso Kopp c. Suiza, (párrafos 74 y ss).; de 16 de febrero de 2000, caso Amann c. Suiza, (párrafos 50, 55 y ss.); de 4 de mayo de 2000, caso Rotaru c. Rumania, (párrafos 52 y ss.); 25 de septiembre de 2001, caso P. G. y J. H. c. Reino Unido, (párrafo 38). A ellas ha de añadirse las dos citadas Sentencias Valenzuela c. España y Prado Bugallo c. España (…).

Esta resolución explica que se determina vulneración del artículo 8 CEDH: "cuando quien reclama la protección no es el titular o usuario de la línea telefónica intervenida sino el destinatario de la comunicación (SSTEDH de 24 de agosto de 1998, caso Lambert c. Francia, (párrafos 38 y ss.); de 16 de febrero de 2000, caso Amann c. Suiza, (párrafos 61 y ss.). Y, en particular, poniendo en conexión la protección que el artículo 8 CEDH brinda a los comunicantes con el requisito relativo a la necesaria previsión legal de la injerencia, ha declarado la vulneración de este derecho por ausencia de previsión legal si la legislación "no regula de forma detallada el caso de los interlocutores escuchados 'por azar', en calidad de 'partícipes necesarios' de una conversación telefónica registrada por las autoridades en aplicación de sus disposiciones" (STEDH de 16 de febrero de 2000, caso Amann c. Suiza, párrafo 61). Por último, se ha de recordar también que la ley que habilite la intervención telefónica ha de ser previa al momento en que se autorice (STEDH de 18 de febrero de 2003, Prado Bugallo c. España, párrafo 32)".

Esta jurisprudencia es además reflejo en la Recomendación 2/99 sobre la protección de la intimidad, adoptada el 3 de Mayo de 1999, en el contexto de la interceptación de las telecomunicaciones, por el Grupo de trabajo sobre la protección de las personas en lo que respecta al tratamiento de datos personales. Con el objetivo de "recordar la aplicación de las medidas adoptadas a nivel europeo en cuanto a interceptación de las telecomunicaciones, de los principios de protección de los derechos y libertades fundamentales de las personas físicas, y, en particular, de su intimidad y del secreto de la correspondencia", ponen de relieve los riesgos vinculados a una interceptación de las telecomunicaciones que sobrepase el marco estricto de las cuestiones de seguridad nacional. La Recomendación

se refiere en general tanto al contenido de las comunicaciones como a los datos correspondientes a las telecomunicaciones, y en particular, a posibles "medidas preparatorias (tales como el "monitoring" y el "datamining" de los datos de tráfico) que se pudieran prever con el fin de decidir la oportunidad de la interceptación del contenido de la telecomunicación"[602]. Se considera a las medidas preparatorias de la interceptación como parte de la misma, por cuanto con ellas también pueden verse afectados derechos fundamentales.

La Recomendación recuerda que las interceptaciones afectan tanto al conocimiento por una tercera parte, del contenido de las comunicaciones privadas entre dos o varios corresponsales, como al conocimiento de los datos asociados a las mismas, en particular, de los datos de tráfico vinculados a la utilización de los servicios de telecomunicación. Considera que ese conocimiento constituye una violación del derecho a la intimidad de los individuos y del secreto de la correspondencia y, que solo puede admitirse que la interceptación se realice con respeto al apartado 2 del artículo 8 del Convenio Europeo de Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950, y a tres requisitos:

> 1.- un fundamento jurídico o texto legal, accesible al público y, que deberá definir precisamente los límites y modalidades de su ejercicio, por medio de normas claras y detalladas, necesarias sobre todo debido al perfeccionamiento continúo de los medios técnicos utilizables,
>
> 2.- la necesidad de tal medida en una sociedad democrática,

[602] Este carácter amplio del concepto de interceptación parte de la Resolución del Consejo del 17 de enero de 1995 relativa a la interceptación legal de las telecomunicaciones. La recomendación se aplica a la interceptación de las telecomunicaciones no públicas en Internet y se presta especial atención a la problemática general del tratamiento de datos personales vinculada al desarrollo de la red Internet. La Resolución del Consejo enumera en el artículo 1.4 del Anexo, las condiciones técnicas necesarias para la interceptación de las telecomunicaciones, y prevé una obligación por parte los operadores de redes o proveedores de servicios de proporcionar los datos interceptados. Estos datos abarcan las llamadas telefónicas, móviles o no, los correos electrónicos, los mensajes fax y télex, los flujos de datos Internet, tanto por lo que se refiere al conocimiento del contenido de las telecomunicaciones como de los datos sobre las telecomunicaciones (en particular, los datos de tráfico, pero también todas las señales emitidas por la persona supervisada), en general, los datos se refieren a la persona supervisada, a las personas que la llaman y a las personas a quienes ésta llama, en un objetivo de protección de los intereses nacionales, de seguridad nacional e investigación de crímenes graves.

3.- la conformidad con uno de los objetivos legítimos enumerados en el Convenio[603].

Se rechaza por norma general el control arbitrario y masivo de las telecomunicaciones[604].

Por otra parte, se tienen en cuenta las previsiones de la Directiva 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que viene en general a imponer la obligación de los Estados miembros de proteger el secreto de las comunicaciones por medio de normativas nacionales que garanticen la confidencialidad de las comunicaciones efectuadas a través de redes públicas de telecomunicaciones o de servicios de telecomunicaciones accesibles al público, siguiendo los principios contenidos en el Convenio Europeo de Protección de los Derechos Humanos de 4 de noviembre de 1950 y en el Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales.

En especial, son interesantes las conclusiones con que termina este documento, sobre el respeto de las libertades fundamentales por parte de las autoridades públicas en el ámbito de las interceptaciones, invitando a los gobiernos a que a través del derecho nacional precisen de manera rigurosa:

---

[603] "El Convenio n° 108 del Consejo de Europa prevé que sólo se tolerará una medida de injerencia cuando constituya una medida necesaria en una sociedad democrática para la protección de los intereses nacionales enumerados en el apartado 2 de su artículo 9 (se tendrá en cuenta que los intereses nacionales enumerados en el Convenio 108 y en el Convenio de Protección de Derechos Humanos no son exactamente iguales), y cuando esté estrictamente definida respecto a esta finalidad".

[604] Sentencias del TEDH: STEDH Klass, de 6 de septiembre de 1978, STEDH Leander, de 25 de febrero de 1987 y, STEDH Malone, de 2 de agosto de 1984. Tanto la primera como la segunda, hacen hincapié en la necesidad de "garantías suficientes contra los abusos, ya que un sistema de vigilancia secreta destinado a proteger la seguridad nacional crea el riesgo de minar, o incluso de destruir, la democracia pretendiendo defenderla". El TEDH observa en la sentencia Klass que la existencia de garantías adecuadas y suficientes contra los abusos en materia de interceptación de las comunicaciones, depende de todas las circunstancias de la causa. Considera que las garantías previstas por la legislación alemana no autorizan la vigilancia general y que por tanto no infringen el artículo 8 del Convenio Europeo de Protección de los Derechos Humanos. Estas garantías se basan en que sólo pueden efectuarse medidas de vigilancia cuando ciertos indicios permitan sospechar que alguien proyecta realizar, realiza o ha realizado infracciones graves, que sólo pueden prescribirse si el esclarecimiento de los hechos por otros medios está llamado al fracaso o presenta considerables obstáculos e incluso, en ese caso, la vigilancia sólo podrá referirse a la persona del sospechoso o a las personas presuntamente en contacto con éste.

1.- las autoridades habilitadas para permitir la interceptación legal de las telecomunicaciones,

2.- los servicios autorizados para proceder a las interceptaciones y el fundamento jurídico de su intervención,

3.- las finalidades según las cuales pueden tener lugar tales interceptaciones, que permitan apreciar su proporcionalidad respecto a los intereses nacionales en juego,

4.- la prohibición de cualquier vigilancia exploratoria o general de las telecomunicaciones a gran escala,

5.- las circunstancias y condiciones precisas (por ejemplo elementos de hecho que justifiquen la medida, duración de la medida) a las cuales están sometidas las interceptaciones, en cumplimiento del principio de especificidad al que se supedita toda injerencia en la intimidad de otros,

6.- el respeto de este principio de especificidad, corolario de la prohibición de cualquier vigilancia exploratoria o general, que implica, por lo que se refiere concretamente a los datos de tráfico, que las autoridades públicas no pueden tener acceso a estos datos sino con carácter particular, y no de manera general y proactiva.

7.- las medidas de seguridad por lo que se refiere al tratamiento y el almacenamiento de los datos, y la duración de su conservación,

8.- por lo que se refiere a las personas implicadas de manera indirecta o aleatoria en las escuchas, las garantías particulares referentes al tratamiento de los datos personales: en particular, los criterios que justifican la conservación de los datos, y las condiciones de la comunicación de estos datos a terceros[605],

[605] Estos datos se refieren a personas que en principio no son objeto de las medidas de vigilancia, pero si su interlocutor, y por este motivo se ven afectadas. Se interceptan datos como por ejemplo el número de

9.- la información a la persona supervisada, lo antes posible,

10.- los tipos de recurso que puede ejercer la persona supervisada,

11.- las modalidades de vigilancia de estos servicios por una autoridad de control independiente,

12.- la publicidad (por ejemplo en forma de informes estadísticos regulares) de la política de interceptación de las telecomunicaciones efectivamente practicada,

13.- las condiciones precisas en las que pueden comunicarse los datos a terceros en el marco de acuerdos bilaterales o multilaterales.

Por último, en enero del año 2010, la Agencia Española de Protección de Datos, ha remitido al Ministerio del Interior un informe de conclusiones sobre la inspección relativa a SITEL, realizada por las presiones políticas que el Gobierno estaba sufriendo al haberse detectado que efectivamente, la normativa no era muy clara. Este informe señala entre sus conclusiones que:

- El tratamiento de datos efectuado por SITEL está amparado en el artículo 579 de la LECrim. y en el artículo 33 de la Ley General de Telecomunicaciones, porque así lo consideran las SSTS de 5 de febrero de 2008 (Sala de lo Contencioso-Administrativo) y 5 de noviembre de 2009 (Sala de lo Penal).

- La incorporación de los datos a SITEL, por parte de la operadora requerida, sólo es posible una vez recibida y analizada la preceptiva autorización judicial. "Las Fuerzas y Cuerpos de Seguridad no pueden por sí mismas, introducir información en SITEL".

---

teléfono marcado por la persona supervisada y correspondiente a uno de los progenitores de este último o la localización geográfica de personas en contacto por teléfono móvil con la persona objeto de escucha, datos que en todo caso deben ser tratados con las debidas garantías.

- La actividad de las Fuerzas y Cuerpos de Seguridad "se efectúa exclusivamente en los términos previstos por la autoridad judicial y para la investigación concreta a la que se refiera dicha autorización de interceptación".

- SITEL tiene como objetivo la puesta a disposición de la autoridad judicial, de la información que ésta solicita y permite que sea obtenida mediante la interceptación de las comunicaciones.

- "Los datos contenidos en SITEL son objeto de bloqueo una vez concluida la investigación que motivó la interceptación y ordenada judicialmente la restricción de los accesos al sistema, no pudiendo producirse el acceso a los mismos salvo que sea requerido por dicha autoridad". El borrado físico se produce también a instancia de la autoridad judicial.

- No es preciso informar al afectado sobre el tratamiento de los datos, ni cabe solicitar de ejercicio de los derechos de acceso, rectificación, cancelación y oposición, de conformidad con las previsiones de la LOPD para este tipo de supuestos.

- Finalmente, considera que "SITEL garantiza el cumplimiento de las medidas de seguridad de nivel alto previstas en el RLOPD, debiéndose hacer especial referencia a aquellas relacionadas con el acceso al sistema por los distintos usuarios del mismo y la seguridad del trasporte de los soportes que contengan la información hasta su entrega a la autoridad judicial".

Dichas apreciaciones no entran a justificar directamente la validez de la norma que ampara las interceptaciones, más bien, indirectamente, y en su valoración del proceso de interceptación de las comunicaciones, insisten en aclarar que de hecho, la intervención judicial se produce desde

la primera fase, sin margen a la arbitrariedad de los funcionarios que lo dirigen.

En otro orden de cosas, y ya ateniéndonos al fondo, el aspecto más controvertido ha sido la redacción del artículo 89 del Reglamento de 2005, que explica cómo se realiza el acceso a los datos de tráfico previo a la emisión de la orden judicial ("información previa a la interceptación").

Señala este precepto que "en el marco de la investigación legal a requerimiento de la autoridad judicial o cuando así lo determine una norma con rango legal" (…) "los operadores que presten o estén en condiciones de prestar servicios de comunicaciones electrónicas disponibles al público" (…) "pondrán a disposición de la autoridad que lleve a cabo dicha investigación" (…) "con carácter previo a la interceptación legal", datos de tráfico, como son la identificación del sujeto de la interceptación, la ubicación donde se encuentre un punto de terminación de red al que el operador da servicio, un identificador de punto de terminación de red (dirección), o de terminal, al que el proveedor de servicios de comunicaciones electrónicas da servicio, el código de identificación en caso de que sea el usuario el que active el terminal para la comunicación, o cualquier otra identidad que corresponda al sujeto especificado en la orden de interceptación. Y continúa el siguiente apartado, diciendo que "con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas".

Es decir, que los llamados "agentes facultados", policía judicial o personal del Centro Nacional de Inteligencia habilitado por una autoridad judicial para materializar una interceptación legal, pueden hoy por hoy acceder a este tipo de datos personales, bastando que una ley así lo permita, sin necesidad de esperar una orden judicial que determine en el

caso concreto, qué datos son necesarios y cuales accesorios, incluyendo datos de terceras personas que nada tengan que ver (en principio) con el investigado[606]. Y esto, además, en el marco de una "investigación "legal".

El artículo 11.2.a) de la LOPD, sobre la posibilidad de realizar cesiones de datos sin necesidad de informar o recabar el consentimiento del afectado, señala efectivamente que si la cesión está prevista en una ley, se podrá hacer así, pero en coherencia con el artículo 22.2, debería tenerse en cuenta que "la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas estén limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales". Es decir, por coherencia, debería tenerse en cuenta, que se debe estar en todo caso ante investigaciones "penales", no bastando estar tan sólo en "el marco de la investigación legal"[607], como permite el cuestionado Reglamento de 2005, y que la orden judicial debería ser previa.

---

[606] Informe elaborado por la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, dependiente de la Secretaría de estado de Seguridad, sobre el sistema operativo SITEL a solicitud de la Audiencia Provincial de Madrid, Sección 1, en oficio libre, con número de Identificación único 7015609/2009, Rollo: 31/2009, de fecha 4 de enero de 2011.: "Sobre el punto ñ en que se solicita la explicación detallada de la concreta forma o mecanismo empleado para acceder al número de abonado 664.71.2x.xx, así como a la identidad de su supuesto usuario, responde este informe, diciendo que: Tanto al número de abonado como a la identidad del usuario se accedió a través de fuentes policiales propias". (p. 3). Generalmente, se suele aludir a actuaciones de seguimiento y localización físicas, como parte de la propia investigación.

[607] Véase la famosa Sentencia del TJCE, de 29 de enero de 2008, Sentencia del Tribunal de Justicia en el asunto C-275/06; Productores de Música de España (Promusicae) / Telefónica de España, S.A.U. (DO C 64 de 08.03.2008, p.9), en que bajo la forma de cuestión prejudicial el tribunal español, preguntaba al tribunal europeo: "El Derecho comunitario y, concretamente, los artículos 15, apartado 2, y 18 de la Directiva [2000/31], el artículo 8, apartados 1 y 2, de la Directiva [2001/29], el artículo 8 de la Directiva [2004/48], y los artículos 17, apartado 2, y 47 de la Carta [...], ¿permiten a los Estados miembros restringir al marco de una investigación criminal o para la salvaguardia de la seguridad pública y de la defensa nacional, con exclusión, por tanto, de los procesos civiles, el deber de retención y puesta a disposición de datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, que recae sobre los operadores de redes y servicios de comunicaciones electrónicas, proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamientos de datos? Y la respuesta no pudo ser más clara: Según el artículo 5, apartado 1, de la Directiva 2002/58, la confidencialidad de las comunicaciones también se extiende a los datos de tráfico asociados a ellas. Los Estados miembros están obligados a prohibir, particularmente, la intervención o vigilancia de datos de tráfico por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el artículo 15, apartado 1. Es decir, los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE". El Derecho comunitario no obliga a los Estados miembros a divulgar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil.

En el sentido expuesto, la Sala Segunda de los Penal, del Tribunal Supremo Español, viene a "salvar" interpretaciones de dudosa legalidad, en la Sentencia 247/2010, de 18 de marzo de 2010, reconociendo expresamente la necesidad de una autorización judicial para obtener los datos conservados por los operadores de telecomunicaciones, y distingue dos conceptos:

a) Datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el artículo 18.3 CE[608];

b) Datos o circunstancias personales referentes a la intimidad de una persona (artículo 18.1 CE), pero autónomos o desconectados de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o habeas data del artículo 18.4 CE que no pueden comprometer un proceso de comunicación.

Y recuerda que la Sala General no jurisdiccional, aprobó con fecha 23 de febrero de 2010 un acuerdo por el que se señalaba que "es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio Fiscal necesitará de tal autorización para obtener de los operadores los datos conservados que se especifican en el artículo 3 de la Ley 25/2007 de 18 de octubre[609]."

---

[608] (F.Jº 2º) "A nuestro juicio, sin pretensiones ni mucho menos de sentar doctrina (obiter dicta), los datos identificativos de un titular o de un terminal deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones (artículo 18.3 CE) sino en el marco del derecho a la intimidad personal (artículo 18.1 CE)" con la salvaguarda que puede dispensar la LOPD o su Reglamento, la LGT o su Reglamento, en los que se desprende que "sin el consentimiento del titular de unos datos reservados, contenidos en archivos informáticos, no pueden facilitarse a nadie, salvo los casos especiales que autorizan sus propias normas, entre las que se halla la autorización judicial, que lógicamente estaría justificada en un proceso de investigación penal".

[609] Artículo 3 de la Ley 25/2007: "1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:
a) Datos necesarios para rastrear e identificar el origen de una comunicación:
1.° Con respecto a la telefonía de red fija y a la telefonía móvil:
i) Número de teléfono de llamada. ii) Nombre y dirección del abonado o usuario registrado.
2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:
i) La identificación de usuario asignada. ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía. iii) El nombre y dirección del abonado o del

Por último, y no menos importante, otro aspecto criticado del funcionamiento de SITEL es el volcado de datos y la fiabilidad de las pruebas obtenidas, lo pone de manifiesto el Voto Particular emitido por los Magistrados D. Manuel Marchena Gómez y D. Jose Manuel Maza Martín, en la Sentencia del Tribunal Supremo de fecha 1 de febrero de 2010[610], emitido sobre la efectividad del artículo 230 de la LOPJ, sobre la autenticidad e integridad de la prueba electrónica, para poder desplegar igual validez y eficacia que un documento original. Señalan que la prueba debe estar garantizada mediante el cumplimiento de los requisitos exigidos por las leyes procesales, y que no bastan actos de fe sobre las excelencias del sistema utilizado para obtenerlas o almacenarlas, sea el software utilizado o

---

usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.
b) Datos necesarios para identificar el destino de una comunicación:
1.º Con respecto a la telefonía de red fija y a la telefonía móvil:
i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas. ii) Los nombres y las direcciones de los abonados o usuarios registrados.
2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:
i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet. ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.
c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:
1.º Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.
2.º Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:
i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado. ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.
d) Datos necesarios para identificar el tipo de comunicación.
1.º Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).
2.º Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.
e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:
1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.
2.º Con respecto a la telefonía móvil:
i) Los números de teléfono de origen y destino. ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada. iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada. iv) La IMSI de la parte que recibe la llamada. v) La IMEI de la parte que recibe la llamada. vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.
3.º Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:
i) El número de teléfono de origen en caso de acceso mediante marcado de números. ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.
f) Datos necesarios para identificar la localización del equipo de comunicación móvil:
1.º La etiqueta de localización (identificador de celda) al inicio de la comunicación.
2.º Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.
2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley".

[610] Voto Particular que formula el Excmo. Sr. D. Manuel Marchena Gómez, en la Sentencia recaída en el Recurso de Casación nº 404/2009, al que se adhiere el Excmo. Sr. D. Jose Manuel Maza Martín.

el grado de confianza institucional en el trabajo de las Fuerzas y Cuerpos de Seguridad[611].

Por eso, este voto particular explica que los derechos fundamentales en juego sólo estarán correctamente garantizados, si las pruebas electrónicas garantizan correctamente la autenticidad de su contenido: "el establecimiento de un sistema que garantice, cuando menos, la integridad de cualquier documento electrónico, constituye un prius para la atribución al mismo de plena eficacia probatoria. Así lo ha entendido el legislador español – en sintonía con un imparable proceso de unificación en el ámbito de la Unión Europea – requiriendo esas garantías incluso cuando el documento emana de un fedatario público".

En el caso concreto que resolvía el Tribunal Supremo se cuestiona la eficacia probatoria de los soportes que recogen las comunicaciones interceptadas por SITEL, al momento de recibir el volcado de datos en soportes digitales (DVDs) y, ser entregados en persona por los funcionarios responsables, al Juzgado. Se entiende que en esta fase del sistema de interceptación, pueden producirse manipulaciones intencionadas que quedarían impunes, o al menos, que no serían tomadas en cuenta a la hora de ser utilizado en el proceso judicial que les da origen, y dice: "este es el problema de origen que nos impide avalar el funcionamiento del sistema integrado (SITEL) que, si bien se mira, no lleva su vocación integradora hasta sus últimas consecuencias, pues se olvida de integrar a los órganos jurisdiccionales en el esquema que define su funcionamiento.(...) El SITEL, en fin, convierte a los Juzgados y Tribunales en un punto débil, en una tierra de nadie en que las garantías de seguridad e integridad del documento electrónico se degradan de forma insalvable. Los Jueces de instrucción se transforman así en meros receptores de unos soportes electrónicos cuyo contenido no puede apoyarse en otra garantía que la confianza acrítica en la profesionalidad de los agentes que se los proporcionan".

[611] La Sentencia señala que (...) "la autenticidad del contenido de los discos está fuera de discusión. Si en alguna ocasión las partes personadas estiman que los discos depositarios de la grabación no responden a la realidad, deberán explicar suficientemente en qué basan su sospecha en cuanto que están acusando de un hecho delictivo a los funcionarios que se encargan del control del sistema SITEL".

En primer lugar, los dos Magistrados discrepantes, son conscientes de que debe buscarse "un saludable equilibrio entre el deseo político de implantación de nuevos modelos de gestión procesal y, el realismo que impone el desfase tecnológico de los Juzgados y Tribunales", pero señalan que esto no puede ignorar tecnologías certificadoras muy útiles, que están al alcance de las autoridades, tales como por ejemplo la firma electrónica. La normativa vigente prevé correctamente las garantías que toda prueba electrónica ha de tener: integridad (el soporte no ha sido alterado), autenticidad (la identificación del sujeto al que se atribuyen las conversaciones y del contenido que éstas reflejan), licitud (que han sido obtenidos con respeto a los derechos y libertades fundamentales), y ello se conseguirá mediante un "sellado tecnológico" que permita verificar que los contenidos probatorios no han sido modificados.

En este sentido la Sentencia señala que "en el sistema SITEL se deja huella identificadora del manipulador ya que debe facilitar su clave de identificación para entrar en el disco duro, pero los magistrados discrepantes creen que el control jurisdiccional de las garantías procesales no puede contentarse con la tranquilidad que proporciona que, de producido, se una manipulación, la impunidad no estará garantizada, o con la idea de que siempre habrá tiempo para un ulterior juicio de revisión. Las garantías deben ser inmanentes al sistema, sin que su afirmación pueda quedar postergada a un momento ulterior, una vez detectada su vulneración*".*

Lo cierto es que en la práctica, hoy por hoy, parece que la figura del "juez" participa de todo el proceso y que la calidad de la información almacenada se garantiza con un sistema de firma electrónica avanzada. Según el Informe elaborado por la Comisaría General de policía Judicial del Cuerpo Nacional de Policía, sobre el sistema operativo SITEL, a solicitud de la Audiencia Provincial de Madrid, en el seno de un procedimiento judicial[612], una vez recibido el contenido de la interceptación en el sistema se firma digitalmente, quedando a disposición de los investigadores habilitados. No

[612] Informe elaborado por la Comisaría General de policía Judicial del Cuerpo Nacional de Policía, sobre el sistema operativo SITEL… Op. Cit. p. 4.

se realiza ninguna operación de encriptación de las conversaciones, las medidas de seguridad son:

- El grupo policial correspondiente entregará el mandamiento judicial a los obligados que determine la orden de interceptación, para que la ejecuten enviando la información interceptada al sistema SITEL "mediante canales seguros unidireccionales preestablecidos al efecto". Los Cuerpos Policiales no podrán acceder ni a puntos de red ni a los datos de la operadora.

- Tanto el contenido de llamada como los datos asociados que se envíen después a los centros de recepción de las interceptaciones, serán almacenados a disposición de la autoridad judicial. La entrega al Juzgado, se hace "mediante un sistema de permisos que impide que grupos policiales ajenos a la investigación tengan acceso a la misma" (…).

- "Los ficheros que se reciben de las operadoras conteniendo los datos de las interceptaciones son firmados digitalmente mediante un sistema de firma avanzada y reconocida que cumple con la Ley 59/2003, de 19 de diciembre, de firma electrónica", de forma que así se garantiza la integridad y autenticidad de la información hasta que sea destruida.

- Los grupos de administración de SITEL son los únicos que pueden acceder al contenido y los datos de las llamadas, y habilitar a los funcionarios que corresponda la entrada al sistema, mediante permisos que incluyen la asignación de una clave y un usuario, "creando los propios investigadores un CD o DVD con los archivos de sus interceptaciones obrantes en SITEL". Sólo este personal autorizado podrá intervenir en el proceso de descarga de los archivos y su grabación en el soporte digital.

- Por último, las llamadas telefónicas son grabadas en el sistema central, y sólo se puede acceder a ello en modo lectura. El personal autorizado no puede en ningún momento "paralizar, modificar ni

borrar las grabaciones ni ningún dato procedente de la operadora relativo a las mismas".

Es evidente que en la defensa de los derechos fundamentales en juego, cuando se pone en marcha un sistema de interceptación de comunicaciones, no basta simplemente garantizar la confidencialidad de la información obtenida, ni la intimidad de los sujetos afectados, sino que se debe ir más allá, porque la tecnología permite que otros aspectos como la propia libertad o la presunción de inocencia del afectado, puedan verse gravemente vulnerados.

2.- Videovigilancia.

La videovigilancia consiste en la instalación física de sistemas técnicos que permiten la captación, y en su caso la grabación, de imágenes, y antes de entrar a analizar las razones y los efectos de la utilización de la videovigilancia con fines de seguridad, conviene reseñar la dimensión constitucional de la imagen como derecho fundamental.

La imagen se recoge en el artículo18.1 CE, y se configura su protección como un derecho de la personalidad, derivado de la dignidad humana y, dirigido a proteger la dimensión moral de las personas. Atribuye a su titular el derecho a determinar qué información gráfica, generada por sus rasgos físicos personales, puede tener difusión pública[613].

Según el Tribunal Constitucional, la esencia del derecho a la imagen se traduce en la facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en "impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad —informativa, comercial, científica, cultural, etc.—

[613] Sentencia del Tribunal Constitucional, nº 14/2003, de 30 de Enero de 2003. F.Jº. 5º, relativa a la vulneración de los derechos a la propia imagen y al honor.

perseguida por quien la capta o difunde[614]. Entiende que lo específico del derecho a la imagen, frente al derecho a la intimidad y el derecho al honor, es la protección frente a las reproducciones de la misma que, afectando a la esfera personal de su titular, no lesionan su buen nombre ni dan a conocer su vida íntima. El derecho a la propia imagen pretende salvaguardar un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás; un ámbito necesario para poder decidir libremente el desarrollo de la propia personalidad y, en definitiva, un ámbito necesario según las pautas de nuestra cultura para mantener una calidad mínima de vida humana". Así, se puede poner en relación directa con el derecho a la protección de datos personales, pues "ese bien jurídico se salvaguarda reconociendo la facultad de evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su propio reconocimiento como sujeto individual"[615].

Señala el Tribunal Constitucional que, "en la medida en que la libertad de la persona se manifiesta en el mundo físico por medio de la actuación de su cuerpo y de las circunstancias del mismo, es evidente que con la protección constitucional de la imagen se preserva no sólo el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a través de la imagen[616] (…) sino también una esfera personal. Así pues, lo que se pretende con este derecho, en su dimensión constitucional, es que los individuos puedan decidir qué aspectos de su persona desean preservar de la difusión pública a fin de garantizar un ámbito privativo para el desarrollo de la propia personalidad ajeno a las injerencias externas"[617]. En suma, se preserva el valor fundamental de la dignidad humana.

[614] Sentencias del Tribunal Constitucional, nº 81/2001, de 26 de marzo (F.Jº. 2º), nº 139/2001, de 18 de junio (F.Jº. 4º) y, nº 83/2002, de 22 de abril (F.Jº. 4º).
[615] Sentencias del Tribunal Constitucional, nº 231/1988, de 2 de diciembre (F.Jº. 3º), nº 99/1994, de 11 de abril (F.Jº. 5º), nº 81/2001, de 26 de marzo (F.Jº. 2º), nº 139/2001, de 18 de junio (F.Jº. 4º), nº 156/2001, de 2 de junio (F.Jº. 6º) y, nº 83/2002, de 22 de abril (F.Jº. 4º).
[616] Sentencia del Tribunal Constitucional nº 117/1994, de 25 de abril (F.Jº. 3º).
[617] Sentencias del Tribunal Constitucional nº 81/2001, de 26 de marzo (F.Jº. 2º), nº 139/2001, de 18 de junio (F.Jº. 5º) y, nº 83/2002, de 22 de abril (F.Jº. 4º).

Ahora bien, el desarrollo de la tecnología ha aumentado enormemente las posibilidades de captación y tratamiento de la información personal que ofrecen las imágenes, a través de sofisticados dispositivos de grabación de imagen y sonido y, además se ha aumentado las posibilidades de difusión con Internet, dado que se unen las posibilidades de captación (texto, imagen y sonido) con la interactividad de las redes. El "derecho a la propia imagen, como cualquier otro derecho, no es un derecho absoluto, y por ello su contenido se encuentra delimitado por el de otros derechos y bienes constitucionales"[618], es importante comprender que "la determinación de estos límites debe efectuarse tomando en consideración la dimensión teleológica del derecho, (…) que debe salvaguardarse el interés de la persona en evitar la captación o difusión de su imagen sin su autorización o sin que existan circunstancias que legitimen esa intromisión. Como ocurre "cuando la propia —y previa— conducta de aquél o las circunstancias en las que se encuentre inmerso justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que puedan colisionar con aquél"[619]. Es decir, que "el derecho a la imagen se encuentra delimitado así por la propia voluntad del titular del derecho que es, en principio, a quien corresponde decidir si permite o no la captación o difusión de su imagen por un tercero. No obstante, como ya se ha señalado, existen circunstancias que pueden conllevar que la regla enunciada ceda, lo que ocurrirá en los casos en que exista un interés público en la captación o difusión de la imagen y este interés público se considere constitucionalmente prevalente al interés de la persona en evitarlas. Por ello, cuando este derecho fundamental entre en colisión con otros bienes o derechos constitucionalmente protegidos deberán ponderarse los distintos intereses enfrentados y, atendiendo a las circunstancias concretas de cada caso, decidir qué interés merece mayor protección, si el interés del titular del derecho a la imagen en que sus rasgos físicos no se capten o difundan sin su consentimiento, o el interés público en la captación o difusión de su imagen"[620].

[618] Sentencias del Tribunal Constitucional nº 81/2001, de 26 de marzo (F.Jº. 2º) y nº 156/2001, de 2 de julio (F.Jº. 6º).
[619] Sentencia del Tribunal Constitucional nº 99/1994, de 11 de abril, (F.Jº. 5º).
[620] Sentencia del Tribunal Constitucional nº 156/2001, de 2 de julio (F.Jº. 6º).

En resumen, la dimensión constitucional del derecho a la imagen pretende "que los individuos puedan decidir qué aspectos de su persona desean preservar de la difusión pública, a fin de garantizar un ámbito privativo para el desarrollo de la propia personalidad ajeno a injerencias externas, impidiendo la obtención, reproducción o publicación por un tercero de una imagen que contenga los rasgos físicos de una persona que permita reconocer su identidad"[621].

Y todo ello, en materia de videovigilancia, debe ponerse en relación con los límites propios de la restricción de los derechos fundamentales, en el sentido de que éstos sólo pueden ceder ante los límites que la Constitución expresamente imponga, "o ante los que de manera mediata o indirecta se infieran de la misma al resultar justificados por la necesidad de preservar otros derechos o bienes jurídicamente protegidos"[622].

En un principio la utilización de videocámaras suele venir justificada por motivos de seguridad, pero no siempre son el medio más proporcionado para el fin pretendido, en ocasiones, suponen más un abuso sobre los derechos de los ciudadanos afectados, cuyas imágenes pueden ser captadas, almacenadas y tratadas, que un derecho de quienes se sirven de estos sistemas de protección[623]. En este sentido, ha de tenerse en cuenta que "la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad". Y para comprobar si una medida restrictiva de un derecho fundamental sigue el principio de proporcionalidad, es necesario constatar si cumple tres requisitos o condiciones esenciales: "si la medida es susceptible

[621] Sentencias del Tribunal Constitucional nº 156/2001, de 2 de julio (F.Jº. 7º), nº 83/2002, de 22 de abril (F.Jº. 4º).
[622] Sentencias del Tribunal Constitucional nº 11/1981, de 8 de abril (F.Jº. 7º) y nº 2/1982, de 29 de enero (F.Jº. 5º).
[623] "La autodeterminación del individuo presupone...que se conceda al individuo la libertad de decisión sobre las acciones que vayan a realizar o, en su caso, a omitir... El que no pueda percibir con seguridad suficiente que informaciones relativas a éste son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse substancialmente cohibido en su libertad de planificar o decidir por autodeterminación... Quien sepa se antemano que su participación, por ejemplo, en una reunión o iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales... De este modo un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo la elaboración automática de datos, ninguno" sin interés". Sentencia del Tribunal Constitucional Federal Alemán, sobre la Ley del Censo Alemana, de 15 de Diciembre de 1983. Boletín de Jurisprudencia Constitucional, Nº 33, Enero, 1984. p. 153.

de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"[624]. Por tanto, la decisión de instalar sistemas de vigilancia por videocámara ha de ser siempre proporcionada a los diferentes fines a que puede servir, como la protección de las personas físicas, la protección de la propiedad, la protección del interés público, la detección, prevención y control de delitos o la puesta a disposición de pruebas para ello[625].

En España, por primera vez se puso de manifiesto la importancia de la instalación de dispositivos de videovigilancia con motivos de seguridad, para la opinión pública, a partir de un suceso clave. En Agosto de 1993, durante las fiestas de Bilbao, se produjo el linchamiento del agente del Ertzaintza Ander Susaeta[626], hecho que fue captado por cámaras de videovigilancia y cuyas imágenes sirvieron de prueba definitiva para la condena de los agresores[627].

Esta circunstancia forjó una corriente de opinión a favor de estos sistemas, llegando al Congreso de los diputados el 4 de octubre de 1996, el debate sobre "la prevención de actos delictivos, la protección de las personas y la conservación y custodia de bienes que se encuentren en situación de peligro, y especialmente cuando las actuaciones perseguidas suceden en espacios abiertos al público, lleva a los miembros de las Fuerzas y Cuerpos de Seguridad al empleo de medios técnicos cada vez más

[624] Sentencias del Tribunal Constitucional nº 66/1995, de 8 de mayo (F.Jº. 5º), nº 55/1996, de 28 de marzo (F.Jº. 7º, F.Jº. 8º y F.Jº 9º); nº 270/1996, de 16 de diciembre (F.Jº. 4º.e), nº 37/1998, de 17 de febrero (F.Jº. 8º) y, nº 186/2000, de 10 de julio (F.Jº. 6º).

[625] Introducción del Documento de trabajo relativo al tratamiento de datos personales mediante vigilancia por videocámara, Grupo del artículo 29 sobre protección de datos, de 25 de noviembre de 2002. Disponible en: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm [21 agosto, 2009].

[626] GONZÁLEZ URDÍNGUIO, A. y GONZÁLEZ GUTIERREZ DE LEÓN, Mª A. "La videovigilancia en el sistema democrático español: Análisis y crítica de la Ley Orgánica 4/1997, de 4 de Agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos", *Revista de la Facultad de Derecho de la Universidad Complutense*, Nº 89. 1998. pp. 105-124.

[627] Sentencia de la Audiencia provincial de Bilbao, de 10 de enero de 1997.

sofisticados". Consideró el legislador[628], para concluir con la aprobación de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, que "con estos medios, y en particular mediante el uso de sistemas de grabación de imágenes y sonidos y su posterior tratamiento, se incrementa sustancialmente el nivel de protección de los bienes y libertades de las personas". Era pues el momento oportuno para "proceder a la regulación del uso de los medios de grabación de imágenes y sonidos que vienen siendo utilizados por las Fuerzas y Cuerpos de Seguridad, introduciendo las garantías que son precisas para que el ejercicio de los derechos y libertades reconocidos en la Constitución sea máximo y no pueda verse perturbado con un exceso de celo en la defensa de la seguridad pública".

La Ley Orgánica 4/1997, de 4 de agosto, introdujo una serie de garantías necesarias en el uso de sistemas de grabación de imágenes y sonidos por las Fuerzas y Cuerpos de Seguridad, basadas en el principio de proporcionalidad (idoneidad e intervención mínima), estableciendo un régimen de autorización previa para la instalación de videocámaras que se concede por los órganos administrativos, previo informe de la Comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías[629], que está presidida por el Presidente del Tribunal Superior de Justicia de la Comunidad Autónoma correspondiente.

Pero la utilización de videocámaras puede darse tanto en el ámbito privado como en el público, de forma que si bien las Administraciones públicas tienen perfectamente delimitado el ámbito de actuación, sucede que los particulares (personas físicas o jurídicas), no siempre conocen los riesgos y necesarios límites que deben tener en cuenta a la hora de instalar videocámaras en sus recintos.

---

[628] Preámbulo de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

[629] Real Decreto 1289/1999, de 23 de julio, por el que se crea la Comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías. BOE nº 178, 27 de Julio de 1999: "La idea de sociedad de la información engloba un conjunto de actividades industriales y económicas, comportamientos sociales, actitudes individuales y formas de organización política y administrativa, de importancia creciente en las naciones situadas en la vanguardia económica y cultural, a lo que no pueden sustraerse los poderes públicos".

Respecto del ámbito privado, la Disposición Adicional Novena de la Ley Orgánica 4/1997, de 4 de agosto, establece una habilitación al Gobierno para que en el plazo de un año elaborase "la normativa correspondiente para adaptar los principios inspiradores de la presente Ley al ámbito de la seguridad privada", sin embargo, la instalación de cámaras se sigue ordenando en la Ley 23/1992, de 30 de julio, de seguridad privada, cuyo desarrollado reglamentario se realiza por el RD 2364/1994, de 9 de diciembre, por el que se aprueba el reglamento de Seguridad Privada[630], texto que contiene la referencia específica al uso de videocámaras en el sector privado, específicamente, en el sector bancario[631]. Otra norma que regula la instalación de cámaras de seguridad, el tratamiento de la información que con ello se recoge, es por supuesto la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal.

La videovigilancia es un medio de protección especialmente invasivo, y por ello resulta necesario verificar para su utilización la existencia de una serie de condiciones que den legitimidad a los tratamientos y, de cumplimiento de los principios y garantías que deben aplicarse. Dada la escasa regulación normativa en la que puede basarse para ello el sector privado[632], la Agencia Española de Protección de Datos dictó la Instrucción

---

[630] BOE nº 8, de 10 de enero de 1995.

[631] Artículo 120. Medidas de seguridad concretas.

"1. En los establecimientos u oficinas de las entidades de crédito donde se custodien fondos o valores, deberán ser instalados, en la medida que resulte necesaria en cada caso teniendo en cuenta las circunstancias enumeradas en el artículo 112 de este Reglamento y los criterios que se fijen por el Ministerio de Justicia e Interior, oyendo a la Comisión Mixta Central de Seguridad Privada:

a) Equipos o sistemas de captación y registro, con capacidad para obtener las imágenes de los autores de delitos contra las personas y contra la propiedad, cometidos en los establecimientos y oficinas, que permitan la posterior identificación de aquéllos, y que habrán de funcionar durante el horario de atención al público, sin que requieran la intervención inmediata de los empleados de la entidad.

Los soportes destinados a la grabación de imágenes han de estar protegidos contra robo, y la entidad de ahorro o de crédito deberá conservar los soportes con las imágenes grabadas durante quince días al menos desde la fecha de la grabación, en que estarán exclusivamente a disposición de las autoridades judiciales y de las dependencias de las Fuerzas y Cuerpos de Seguridad, a las que facilitarán inmediatamente aquellas que se refieran a la comisión de hechos delictivos.

El contenido de los soportes será estrictamente reservado, y las imágenes grabadas únicamente podrán ser utilizadas como medio de identificación de los autores de delitos contra las personas y contra la propiedad, debiendo ser inutilizados el contenido de los soportes y las imágenes una vez transcurridos quince días desde la grabación, salvo que hubiesen dispuesto lo contrario las autoridades judiciales o las Fuerzas y Cuerpos de Seguridad competentes".

[632] Como se ha expuesto, existe una escasísima regulación normativa sobre la videovigilancia en el sector privado, y ello a pesar de las actualizaciones introducidas en la Ley 23/1992, de 30 de julio, tanto por el Real Decreto-ley 2/1999, de 29 de enero, como por la Ley 14/2000, de 29 de diciembre, de Medidas fiscales, administrativas y del orden social y, por el Real Decreto-ley 8/2007, de 14 de septiembre, por el que se modificaron los artículos 1, 7, 9 y 10 de la referida Ley de Seguridad Privada.

1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras[633].

Esta Instrucción se entiende necesaria en ese momento porque "el incremento que últimamente están experimentando las instalaciones de sistemas de cámaras y videocámaras con fines de vigilancia ha generado numerosas dudas en lo relativo al tratamiento de las imágenes que ello implica. Además es un sector que ofrece múltiples medios de tratar datos personales como pueden ser los circuitos cerrados de televisión, grabación por dispositivos "Webcams", digitalización de imágenes o instalación de cámaras en el lugar de trabajo". Asimismo, se pretende dejar claro que "la seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático".

La esencia de las recomendaciones que se recogen en dicho texto, determina que "toda instalación de cámaras de vigilancia, deberá respetar el principio de proporcionalidad"[634], y éste se cumplirá si se dan simultáneamente tres requisitos: "si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

Para la instalación de cámaras de videovigilancia en el sector privado, sin que sean invadidas las competencias propias de las autoridades

[633] Las imágenes se consideran un dato de carácter personal, en virtud del artículo 3 de la Ley Orgánica 15/1999 y del artículo 1.4 del Real Decreto 1322/1994 de 20 de junio, que considera como dato de carácter personal "la información gráfica o fotográfica".

[634] Respecto de la "proporcionalidad", la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de "una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad".

policiales, se debe tener en cuenta que dichas instalaciones no pueden ser ubicadas en las vías públicas (pues la seguridad en las vías públicas queda fuera del ámbito de actuación de la seguridad privada, salvo casos excepcionales)[635], y que en todo caso tendrán como finalidad el incremento o mejora de la seguridad respecto de las personas, bienes, servicios y establecimientos de cuya protección, vigilancia o custodia estuvieren encargadas. Y es que la seguridad pública es una función específicamente encomendada a las Fuerzas y Cuerpos de Seguridad[636]. Por tanto, siendo éstas las únicas competentes para garantizar la seguridad ciudadana en los lugares públicos, la normativa sobre seguridad pública no podrá en ningún caso servir de base a las empresas de seguridad privada, ni en el ejercicio de sus funciones, ni en lo referente a medios personales y materiales para el cumplimiento de las mismas[637].

Y esto es así, lógicamente, en aras del control de la instalación de cámaras por empresas de seguridad privada, y el respeto de esas pautas básicas en tratamiento de datos personales en forma de imagen. La Ley 23/1992, de 30 de julio, de Seguridad Privada en su Exposición de Motivos establece claramente que:

> "La proyección de la Administración del Estado sobre la prestación de servicios de seguridad por empresas privadas y sobre su personal se basa en el hecho de que los servicios que prestan forman parte del núcleo esencial de la competencia exclusiva en materia de seguridad pública atribuida al Estado por el artículo 149.1.29 de la Constitución, y en la misión que, según el artículo 104 del propio texto fundamental, incumbe a las Fuerzas y Cuerpos de Seguridad, bajo la dependencia del Gobierno, de proteger el libre ejercicio de los derechos y libertades y garantizar la

[635] Informe nº 13, sobre seguridad privada, de la Secretaría General Técnica del Ministerio del Interior, sobre los requisitos exigibles a las empresas instaladoras de sistemas de videocámaras para su autorización e inscripción. Disponible en: http://www.interior.gob.es/file/52/52779/52779.pdf

[636] Artículo 1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

[637] La Ley Orgánica 4/1997, ha establecido el marco jurídico aplicable a la utilización de los sistemas de grabación de imágenes y sonidos en lugares públicos, como medio del que pueden servirse las citadas Fuerzas y Cuerpos de Seguridad en el cumplimiento de su misión de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.

> seguridad ciudadana. (...) La defensa de la seguridad no puede ser ocasión de agresiones, coacciones, desconocimiento de derechos o invasión de las esferas jurídicas y patrimoniales de otras personas. Y ésta es una de las razones que justifican la intensa intervención en la organización y desarrollo de las actividades de las empresas privadas de seguridad, por parte de las Fuerzas y Cuerpos de Seguridad del Estado, que tienen la misión constitucional de proteger los derechos fundamentales de todos los ciudadanos y garantizar su seguridad".

Las Fuerzas y Cuerpos de Seguridad del Estado tienen la obligación de supervisar el desarrollo de las actividades privadas de seguridad, y así, el control de las actividades de videovigilancia en el sector privado lo tiene directamente el Ministerio del Interior[638], a través Registro General de Empresas de Seguridad, y los Registros Autonómicos en aquellas Comunidades Autónomas que tengan competencia para ello. Estos registros funcionan dentro de una unidad orgánica especializada en materia de seguridad privada, la Unidad Central de Seguridad Privada[639], que es parte de la organización la Comisaría General de Seguridad Ciudadana, y que se encarga de la autorización, inscripción y registro de nuevas empresas de seguridad. La Comisaría General de Seguridad Privada es en general la entidad que se encarga directamente de "la organización y gestión de lo relativo a la prevención, mantenimiento y, en su caso, restablecimiento del orden y la seguridad ciudadana; el control de las empresas y del personal de la seguridad privada; la vigilancia de los espectáculos públicos, dentro del ámbito de competencia del Estado, y la protección de altas personalidades, edificios e instalaciones que por su interés lo requieran"[640].

[638] Artículo 7 de la Ley 23/1992, de 30 de julio, de Seguridad Privada y Disposiciones Adicionales Segunda y Tercera, del Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.

[639] Más información sobre la Comisaría General de Seguridad Ciudadana, disponible en su página web: http://www.policia.es/cgsc/index.htm [22 agosto 2009].

[640] Artículo 3. A) 3. c) del Real Decreto 1181/2008, de 11 de julio, por el que se modifica y desarrolla la estructura orgánica básica del Ministerio del Interior.

Respecto del sistema de autorizaciones vigente para instalación de cámaras de seguridad en lugares privados, en alguna ocasión se ha criticado la centralización geográfica de los Registros de Empresas de Seguridad, por cuanto podría ser mucho más efectivo que fuesen los municipios, los propios Ayuntamientos, quienes se ocupasen de otorgar las licencias, previo control directo del cumplimiento de los requisitos legalmente exigibles para la instalación de las videocámaras, de tal forma que incluso podrían llegar a ser considerados como responsables subsidiarios en caso de que la empresa en cuestión incurriese en la vulneración de derechos fundamentales de los ciudadanos afectados[641].

2.1.- Normativa española para el Sector Público.

En general, se puede decir que el sector público dispone de normativa específica, clara y precisa, que establece las directrices de la instalación de cámaras de seguridad y, del tratamiento que puede hacerse de las imágenes captadas, mientras que el sector privado, de momento, se guía básicamente por la Ley 23/1992, de 30 de julio, de Seguridad Privada y, por las recomendaciones de la Agencia Española de Protección de datos. De hecho, la Instrucción 1/2006, de 8 de noviembre, aunque lo reconoce en relación con el sector de la seguridad privada, excluye de su ámbito de aplicación el tratamiento de imágenes utilizado "para el ejercicio de sus funciones por parte de las Fuerzas y Cuerpos de Seguridad, que está cubierto por normas específicas (aunque estos tratamientos también deberán cumplir las garantías establecidas por la Ley Orgánica 15/1999)". La Ley Orgánica 15/1999, de 13 de diciembre, establece por su parte, en su artículo 2.3 que "se regirán por sus disposiciones específicas, y por lo

[641] SALDAÑA SOLERA, J. "Videovigilancia y Protección de Datos Personales". *Revista Ayuntamiento XXI, Editorial Difusion Jurídica y Temas de Actualidad S.A.* Nº 20 - 2º Trimestre de 2006, p. 38.

especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales: Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia".

La Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, pone de manifiesto en su primer artículo que el objeto de la regulación que contiene es sin más "la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública. Asimismo, esta norma establece específicamente el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de respetarse ineludiblemente en las sucesivas fases de autorización, grabación y uso de las imágenes y sonidos obtenidos conjuntamente por las videocámaras*".* Y precisa además que todas las referencias a videocámaras, cámaras fijas y cámaras móviles que contiene en su articulado, se deben entender "hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas".

Este precepto trata de salvaguardar posibles incidencias en materia de derechos fundamentales, anunciando lo que más adelante dispone el artículo 6, sobre la necesidad de establecer un límite entre la protección de la seguridad pública y la invasión de la intimidad de los ciudadanos afectados, entendida en sentido amplio. Ese límite es en todo caso la proporcionalidad, en su doble versión: de idoneidad e intervención mínima. Explica que la "idoneidad" significa que "sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley y que la "intervención mínima", exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de

la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas". Es más, expresamente se dice que "la utilización de videocámaras exigirá la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles".

Es decir, el legislador se ocupó de recoger la más que evidente incidencia de la videovigilancia en los derechos consagrados por el artículo 18 CE, tutelando posibles vulneraciones bajo un régimen especial de tratamiento de datos personales en forma de imagen, por las Fuerzas de Seguridad del Estado y, en relación con el bien jurídico "seguridad pública", cuando "se afecte de forma directa y grave la intimidad de las personas", incluyendo prohibiciones expresas como la grabación de conversaciones de "naturaleza estrictamente privada" o, tomar imágenes o sonidos del interior de las viviendas y de sus vestíbulos, salvo consentimiento del titular o autorización judicial[642].

Por otra parte, el artículo 2 de esta norma, confirma lo antes dicho cuando señala expresamente que "la captación, reproducción y tratamiento de imágenes y sonidos, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo", es decir, cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso.

Esto es así, porque el legislador toma el "honor" como la cualidad moral que lleva al cumplimiento de los propios deberes respecto del prójimo y de uno mismo[643], y que nuestros propios actos, respecto de nosotros mismos, van a ser los que determinen el respeto que esperamos de terceros a determinadas parcelas de nuestra vida, como la intimidad personal y familiar. Así, aquello que mantengamos de hecho lejos de las miradas

[642] Artículo 6.5 de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
[643] Definición de "honor" tomada de la vigésima segunda edición del Diccionario de la Lengua Española, de la Real Academia.

ajenas, como parte de nuestra esfera privada, habrá de mantenerse en principio resguardado de injerencias ajenas. Es en definitiva, el derecho a decidir sobre nuestra propia información personal.

Por otra parte, no hay que olvidar que el legislador establece que la finalidad de la captación de las imágenes, por las Fuerzas de Seguridad del Estado, va a ser la que marque la necesidad de su tratamiento e incluso, el que sea ordenado por una autoridad judicial, como expresión de la voluntad del Estado[644].

Parece que en cuestión de defensa de los derechos consagrados por el artículo 18 de la CE, se contienen las previsiones necesarias, pues la Ley 4/1997, de 4 de agosto, contiene incluso una remisión a la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 2.2, al establecer que "sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal". Esta remisión podría considerarse muy acertada al referirse a la norma específica que protege el tratamiento de la información de carácter personal, sin embargo, no se ha tenido en cuenta a la hora de preverla que la propia Ley 15/1999, de 13 de diciembre, sólo se considera a si misma aplicable de forma subsidiaria[645] a los tratamientos de datos personales "procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia (artículo 2.3.e)", porque han de regirse por su normativa específica (remitiéndose así de nuevo a la Ley 4/1997, de 4 de agosto), y no contiene ninguna disposición específica en materia de videovigilancia, por lo que cabe deducir lo difícil que resultará

[644] "Ahora bien, condenar al conjunto de la ciudadanía a una vida vigilada por ojos electrónicos, sobre la base de una decisión estratégica de política criminal, pretendidamente adecuada a la situación específica del País Vasco, parece cuando menos arriesgada. Es más, el empleo de estas técnicas puede situar a los responsables policiales frente a la necesidad de adoptar decisiones en la frontera de los derechos fundamentales y es posible que incida en el comportamiento cotidiano de muchos ciudadanos". MARTÍNEZ MARTÍNEZ, R. *Tecnologías de la Información, Policía...* Op. Cit. p. 394.

[645] Artículo 2.3 de la Ley 15/1999, de 13 de diciembre: "Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales: e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia".

aplicar a un caso concreto, y de forma subsidiaria, la Ley de Protección de Datos a este tipo de tratamientos.

Siguiendo la teoría de Ricard Martínez Martínez[646], sobre posibles interpretaciones a esta situación, se puede considerar bien que los registros de imágenes y sonidos realizados por las Fuerzas y Cuerpos de Seguridad, quedan totalmente fuera del régimen de la LOPD, o bien, que cualquier tratamiento de datos personales realizado a partir de las imágenes y sonidos obtenidos por las Fuerzas y Cuerpos de Seguridad, debe regirse por esta norma, dado que aunque la Ley de Videovigilancia determina específicamente los requisitos tanto para el uso de videocámaras y las condiciones para la captación de las imágenes, como para el uso de éstas y los criterios para el acceso de los ciudadanos a las mismas, no establece prácticamente nada sobre su potencial tratamiento, pudiendo entrar juego la aplicación de la LOPD, de una forma coherente incluso con su definición de "dato personal[647]".

En cualquier caso, y al margen de las anteriores consideraciones sobre la aplicabilidad de la normativa vigente, es preciso analizar, aunque sea someramente, los efectos de la Ley 4/1997, de 4 de agosto, en relación con los tratamientos de imágenes con información de carácter personal, por parte de las Fuerzas y Cuerpos de Seguridad del Estado.

Tanto la Ley de Videovigilancia como su Reglamento de desarrollo, aprobado por el Real Decreto 596/1999, de 16 de abril, han establecido un marco jurídico aplicable a la utilización de los sistemas de grabación de imágenes y sonidos, como medio del que pueden servirse las Fuerzas y Cuerpos de Seguridad en el cumplimiento de la misión encomendada por el artículo 104 de la CE, de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. Y prevén además, su subsidiariedad, en caso de existir disposiciones especificas "de las

[646] MARTÍNEZ MARTÍNEZ, R. *Tecnologías de la Información, Policía...* Op. Cit. p. 338.
[647] Artículo 3.a. de la Ley 15/1999, de 13 de diciembre. – Definición de datos de carácter personal: "cualquier información concerniente a personas físicas identificadas o identificables".

Comunidades Autónomas con competencias para la protección de las personas y los bienes y para el mantenimiento del orden público"[648].

Estas normas exigen que, para la utilización de cámaras de videovigilancia fija, se cuente con la autorización del Delegado del Gobierno en la Comunidad Autónoma de que se trate, previo informe de una Comisión, cuya presidencia corresponderá al Presidente del Tribunal Superior de Justicia de la misma Comunidad[649]. Para la instalación de cámaras móviles, se estará a lo dispuesto por el máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad, quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación para determinar su autorización[650].

Para autorizar la instalación de videocámaras se tendrá en cuenta en todo caso, conforme al principio de proporcionalidad, que las finalidades principales sean las de asegurar la protección de los edificios e instalaciones públicas y de sus accesos, o salvaguardar las instalaciones útiles para la defensa nacional, o constatar infracciones a la seguridad ciudadana, o bien prevenir la causación de daños a las personas y bienes.[651]

Para supervisar el correcto funcionamiento de estas instalaciones, se crearon las Comisiones de garantías de la videovigilancia[652], a las que corresponden las siguientes competencias:

a) Emitir un informe preceptivo sobre las solicitudes de instalaciones fijas de videocámaras, que será vinculante cuando se considere que la instalación podría suponer una vulneración de los criterios de proporcionalidad (artículo 4 LO 4/1997), en cuyo caso, no podrá concederse la autorización solicitada. También será vinculante cuando, siendo favorable a la instalación, se condicione

[648] Disposición Adicional Primera del Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
[649] Artículo 3 de la Ley Orgánica 4/1997, de 4 de agosto.
[650] Artículo 5 de la Ley Orgánica 4/1997, de 4 de agosto.
[651] Artículo 4 de la Ley Orgánica 4/1997, de 4 de agosto.
[652] Artículo 16 del Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto.

a restricciones, limitaciones o prevenciones en orden al cumplimiento de dichos criterios de proporcionalidad.

b) Ser informada de las resoluciones de autorización de videocámaras móviles y del uso excepcional de las mismas, previstos en el apartado 2 del artículo 5 de la Ley Orgánica 4/1997[653].

c) Ser informada, al menos con periodicidad quincenal, de la utilización que se haga de videocámaras móviles.

d) Recabar en cualquier momento, de las Fuerzas y Cuerpos de Seguridad, el soporte físico de las grabaciones efectuadas por videocámaras móviles y emitir un informe al respecto.

e) Informar, a petición de las autoridades competentes, sobre la adecuación de cualquier registro de imagen y sonido obtenidos mediante videocámaras móviles a los principios enunciados en el artículo 6 de la Ley Orgánica 4/1997[654].

f) Ordenar la destrucción de las grabaciones cuando, en el ejercicio de sus competencias, constaten el incumplimiento de los criterios y principios establecidos en la Ley.

g) Requerir de las autoridades responsables la información necesaria para el ejercicio de sus funciones.

h) Formular cuantas recomendaciones estime oportunas en el ámbito de sus competencias.

---

[653] Artículo 5.2 de la LO 4/1997, de 4 de agosto: "En casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización indicada en razón del momento de producción de los hechos o de las circunstancias concurrente, se podrán obtener imágenes y sonidos con videocámaras móviles, dando cuenta, en el plazo de setenta y dos horas, mediante un informe motivado, al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión aludida en el párrafo anterior, la cual, si lo estima oportuno, podrá requerir la entrega del soporte físico original y emitir el correspondiente informe".

[654] Se refiere a los principios de proporcionalidad, en su doble versión de idoneidad y de intervención mínima, a la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las cámaras fijas, o de un peligro concreto, en el caso de las cámaras móviles y, a la inviolabilidad del domicilio (respeto del derecho a la intimidad), salvo consentimiento del titular o autorización judicial.

Este conjunto de competencias permiten no sólo un control previo del uso de las cámaras, sino también la posibilidad de supervisar a posteriori el tratamiento de la información que recaben, ordenando en su caso la destrucción de todas las grabaciones. Es más, si la Comisión detecta la realización de una de las infracciones previstas por la Disposición Adicional Séptima de la Ley de Videovigilancia o de un ilícito penal deberá ponerlo en conocimiento de la autoridad judicial o administrativa correspondiente conservándose en este caso las imágenes a fin de permitir la pertinente práctica de la prueba[655]. A pesar de ello, no tienen encomendadas funciones que les permitan expresamente velar por la protección de datos personales de los ciudadanos, en cuyo caso se entiende, habrá de acudirse a la tutela de la Agencia Española de Protección de Datos y/o de los Tribunales.

En cuanto a los derechos de los ciudadanos, se respeta su ejercicio partiendo del básico derecho a la información. El artículo 9 de la Ley 4/1997, de 4 de agosto, establece que:

> "1. El público será informado de manera clara y permanente de la existencia de videocámaras fijas, sin especificar su emplazamiento, y de la autoridad responsable.
>
> 2. Toda persona interesada podrá ejercer los derechos de acceso y cancelación de las grabaciones en que razonablemente considere que figura. No obstante, el ejercicio de estos derechos podrá ser denegado por quien custodie las imágenes y sonidos, en función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se están realizando".

El Reglamento por su parte, concreta las opciones de ejercicio de estos derechos señalando en los artículos 21 y siguientes que, partiendo de que "la información al público de la existencia de instalaciones fijas de

[655] Artículos 18 y 19 del Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto.

videocámaras será responsabilidad de la autoridad que haya otorgado la autorización, y deberá ser efectiva desde el mismo momento en que se proceda a la utilización de las mismas, debiendo mantenerse actualizada de forma permanente", deberá contener en todo caso una descripción genérica de la zona de vigilancia y de las autoridades responsables de la autorización y custodia de las grabaciones, aunque no especificará el emplazamiento concreto de las instalaciones fijas de videocámaras.

Para hacer llegar a los ciudadanos esta información sobre la instalación cámaras fijas, es preceptivo utilizar una placa informativa con el pictograma de una cámara de vídeo, y un panel complementario con el contenido especificado en el artículo anterior. El diseño y formato de la placa informativa y el del panel complementario se especifican en un anexo del propio Reglamento, y en especial se refiere a que debe contener información relativa al responsable de la custodia de las grabaciones.

Una vez que esta información está a disposición de los ciudadanos, habrá de procurarse que el derecho de acceso a las grabaciones sea real, ya que "toda persona que considere razonablemente que figura en grabaciones efectuadas con videocámaras, podrá ejercer el derecho de acceso a las mismas, mediante solicitud dirigida a la autoridad encargada de su custodia". La autoridad competente para la custodia de las grabaciones dispone de un plazo de 10 días para notificar su decisión sobre la petición de acceso al interesado, o bien responder afirmativamente mediante la figura del silencio administrativo. El sistema ordinario de acceso a las grabaciones podrá ser la simple visualización en pantalla.

En el mismo sentido, el afectado puede solicitar la cancelación de las grabaciones cuando considere que las imágenes y sonidos no son ajustadas a lo previsto en la Ley Orgánica 4/1997. En ocasiones, puede que no sea posible o que no se estime conveniente su destrucción total, tanto por razones técnicas, como por causa del procedimiento o soporte utilizado la cancelación parcial de las grabaciones, en cuyo caso, el responsable de su custodia procederá en función de las disponibilidades técnicas, a la distorsión o bloqueo, general o puntual, de las imágenes y, en su caso, de

los sonidos, con el fin principal de impedir su ulterior utilización, sin que ello implique, necesariamente, la supresión o borrado de las restantes imágenes o sonidos.

Ya hemos visto que en esencia la Ley 4/1997, de 4 de agosto, supone un límite al derecho a la intimidad y a la propia imagen de los ciudadanos, por motivos de seguridad pública, sin embargo, éstos no son los únicos derechos afectados a tener en cuenta. Existen límites a otros derechos, derechos afectados pero que pertenecen a personas que no tienen por que ser las afectadas en un primer momento. Se trata de los derechos de los propietarios o titulares de derechos reales sobre bienes afectados por las instalaciones de cámaras, o quienes los posean por cualquier título, ya que están obligados a facilitar y permitir la colocación y mantenimiento de las cámaras[656].

También afecta la cuestión de los plazos, ya que cuanto menor sea el tiempo de conservación de las imágenes captadas, menores serán las posibilidades de intromisión en los derechos de estos afectados. En principio, se ha estimado que un plazo de un mes es proporcionado a los fines que se pretenden, de forma que una vez transcurrido este tiempo desde su captación, habrá de procederse a la destrucción del material captado, salvo que esté relacionado "con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto"[657]. Esta excepción, así redactada, es tal vez demasiado amplia, de forma que puede llegar a posibilitar la conservación indefinida de las imágenes y, lo que es

[656] Disposición Adicional Sexta de la Ley 4/1997, de 4 de agosto.

[657] Artículo 8 de la Ley 4/1997, de 4 de agosto. Conservación de las grabaciones.
"1. Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.
2. Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley.
3. Se prohíbe la cesión o copia de las imágenes y sonidos obtenidos de conformidad con esta Ley, salvo en los supuestos previstos en el apartado 1 de este artículo.
4. Reglamentariamente la Administración competente determinará el órgano o autoridad gubernativa que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior destino, incluida su inutilización o destrucción. Dicho órgano será el competente para resolver sobre las peticiones de acceso o cancelación promovidas por los interesados".

aún peor, la incertidumbre sobre contenido del material conservado en manos del Estado.

En todo caso, en el supuesto de grabaciones ilegales, el responsable de la custodia de las grabaciones deberá destruir de inmediato las imágenes y sonidos obtenidos[658]. Es decir, deberá destruirse la grabación obtenida cuando se haya realizado vulnerando los criterios para la utilización de videocámaras móviles, o cuando se hayan tomado sin consentimiento del titular o la autorización judicial imágenes o sonidos del interior de las viviendas o de sus vestíbulos o las registradas en lugares públicos, abiertos o cerrados, cuando se afecte de forma directa y grave la intimidad de las personas, y finalmente, cuando se hayan grabado conversaciones de naturaleza estrictamente privada[659].

En general, la destrucción del material "podrá hacerse efectiva por cualquier modalidad que permita el borrado o inutilización de las grabaciones, o de las imágenes y sonidos concretos que deban ser cancelados"[660].

Por último, una breve referencia a la excepción prevista por el artículo 2.2 del Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, porque excluye de su ámbito de aplicación la utilización de instalaciones fijas de videocámaras cuando son utilizadas por las Fuerzas Armadas en sus propios inmuebles y, el uso de estos medios por la Policía Judicial. La Disposición Adicional Única, explica que "en el caso de que dicha utilización se realice por las Unidades de Policía Judicial en sentido estricto, se estará a lo dispuesto en la Ley de Enjuiciamiento Criminal y en su normativa específica".

---

[658] Artículo 20 del Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto.

[659] Artículo 6. 5 de la Ley Orgánica 4/1997, de 4 de agosto: "No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares incluidos en el artículo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia".

[660] Artículo 18 del Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto.

Las competencias para controlar la correcta aplicación de estas previsiones, están en manos de las Comisiones de Garantías de la Videovigilancia, de los organismos administrativos que en su caso hayan solicitado la preceptiva autorización al Delegado del Gobierno, para la instalación de las cámaras y, subsidiariamente, el Ministerio del Interior. Pero, en lo que directamente atañe a los derechos de los ciudadanos, aunque la Agencia Española de Protección de Datos carece de competencias para aprobar la instalación de sistemas de cámaras y videocámaras, si puede entrar a valorar que el tratamiento que de las imágenes como dato personal se realice, al amparo de la Ley Orgánica 15/1999, y su Instrucción 1/2006, de 8 de noviembre de 2006, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. En consecuencia, ha emitido una serie de informes jurídicos que se consideran de interés en el estudio de la materia que nos ocupan, por cuanto responden a consultas sobre la instalación de cámaras por los Ayuntamientos y por la Policía Local[661].

En todos estos informes, la Agencia insiste en aclarar su parcela de competencia en la materia y, la normativa aplicable a las consultas que se le plantean, coincidiendo siempre en señalar que "la instalación de cámaras en espacios públicos, es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad del Estado, por aplicación de la Ley Orgánica 4/1997, y por ello queda excluido del ámbito de la Instrucción 1/2006". Así lo determina el artículo 1 en sus dos apartados, en el primero, señalando que el objeto de dicha Ley es regular "la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública". Y en el segundo, señalando que "El tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de

[661] Se destacan los Informes Jurídicos nº 0116/2008, sobre si la instalación de cámaras de video para vigilar las instalaciones de titularidad municipal, requiere de una autorización administrativa previa; nº 0148/2008, sobre grabaciones instaladas y visionadas por la Policía Local; nº 377/2008, sobre el deber de informar sobre grabaciones responsabilidad de la Policía Local y, nº 0286/2009, sobre la finalidad de la instalación de sistemas de videovigilancia en dependencias policiales.

cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad se regirá por las disposiciones sobre la materia. En consecuencia, sí las cámaras graban la vía pública deberá de dirigirse a la Delegación del Gobierno a los efectos de obtener autorización para la instalación de las mismas".

Es interesante mencionar una de las consultas respondidas en el Informe Jurídico 286/2009. Se plantea si las grabaciones obtenidas a través del sistema de videovigilancia instalado en las dependencias de la policía local, pueden ser utilizadas como medios de prueba para exigir a los policías responsabilidades disciplinarias.

Sobre este punto, la Agencia responde que "carece de competencias para valorar qué pruebas o no pueden aportarse en un procedimiento disciplinario, pero dice que, no obstante, según la finalidad declarada en el Registro General de Protección de Datos, el fichero creado es para controlar y vigilar el acceso al edificio, por ello, si las responsabilidades disciplinarias, fueran derivadas del acceso al mismo (horario de entrada y salida por parte de los policía) sí podrían ser utilizadas, no pudiendo ser utilizadas para otro tipo de finalidades, que no consten declaradas". En el año 2003 el Tribunal Europeo de Derechos Humanos, se pronunció en este sentido en el asunto conocido como "Asunto Perry contra el Reino Unido", que se analizará en el siguiente apartado, sobre la normativa europea en materia de videovigilancia.

En territorio español, además de la ya citada Sentencia de la Audiencia Provincial de Bilbao, de fecha 10 de enero de 1997, en el asunto del Ertzaintza Ander Susaeta, cabe mencionar la Sentencia nº 1733/2002 del Tribunal Supremo, de 14 de octubre de 2002, en cuyo Fundamento de Derecho Único, desestima el recurso que le da origen, entendiendo que no existe vulneración del derecho de presunción de inocencia (articulo 24.2 de la CE) por cuanto la actividad probatoria, que se ha basado en la utilización por las autoridades policiales de un sistema de videovigilancia instalado en el exterior de una comisaría, es perfectamente válida. Recoge para ello los argumentos de otras muchas Sentencias dictadas por el Alto Tribunal en

este mismo sentido respecto de la captación de imágenes con motivos de seguridad pública.

La jurisprudencia ha estimado legítimo, porque no se vulneran con ello derechos fundamentales, la actividad de filmación de escenas, presuntamente delictivas, que sucedan en vías o espacios públicos, sin embargo, si considera necesaria autorización judicial para la captación clandestina de imágenes o de sonidos en domicilios o lugares privados[662]. "Así, en la Sentencia de 6 de mayo de 1993 se expresa que las tareas de investigación de todo hecho delictivo están encaminadas a practicar las diligencias necesarias para comprobar y descubrir a los delincuentes y recoger todos los efectos, instrumentos o pruebas del delito, poniéndolos a disposición de la autoridad judicial. En el desarrollo de estas funciones se pueden realizar labores de vigilancia u observación de lugares o personas que pudieran estar relacionadas con el hecho que es objeto de la investigación".

Estas tareas de vigilancia pueden ser desarrolladas en las vías públicas, siguiendo o visualizando conductas de personas consideradas como sospechosas y, para ello, se pueden utilizar "toda clase de medios que permitan constatar la realidad sospechada y que sean aptos para perfilar o construir un material probatorio que después pueda ser utilizado para concretar una denuncia ante la autoridad judicial. Los sistemas de grabación de imágenes deben utilizarse dentro de los márgenes marcados por el respeto a la intimidad y a la inviolabilidad del domicilio".

En general, los derechos establecidos por la Ley Orgánica 1/1982, de 5 de mayo, reguladora de la Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, no pueden considerarse absolutamente ilimitados, ya que imperativos de interés público pueden hacer que se autoricen expresamente por ley determinadas entradas en el ámbito de la intimidad, y que en este sentido, podrán ser reputadas legítimas. De hecho, no podrán ser reputadas "intromisiones ilegítimas" las

[662] Sentencias del Tribunal Supremo de 6 de mayo de 1993; de 7 de febrero, de 6 de abril y de 21 de mayo de 1994; de 18 de diciembre de 1995; de 27 de febrero de 1996; de 5 de mayo de 1997; STS nº 968/98 de 17 de Julio, STS 188/1999, de 15 de febrero y STS nº 1207/1999, de 23 de julio, entre otras.

actuaciones autorizadas o acordadas por la autoridad competente de acuerdo con la ley[663]. Por otra parte el artículo 282, de la Ley de Enjuiciamiento Criminal, autoriza a la Policía Judicial a "practicar las diligencias necesarias para comprobar los delitos y descubrir a los delincuentes", de modo que no existe obstáculo para que las labores de investigación se extiendan a la captación de la imagen de las personas sospechosas, en los momentos en que se supone fundadamente que está cometiendo un hecho delictivo. Del mismo modo que nada se opone a que los funcionarios de Policía hagan labores de seguimiento y observación de personas sospechosas, sin tomar ninguna otra medida restrictiva de derechos, "mediante la percepción visual y directa de las acciones que realiza en la vía pública o en cualquier otro espacio abierto".

Como se ha señalado, la captación de imágenes se encuentra autorizada por la ley en el curso de una investigación criminal, siempre que se limiten a la grabación de lo que ocurre en espacios públicos (fuera del recinto inviolable del domicilio, en respeto del ejercicio del derecho a la intimidad), por tanto, cuando la instalación de sistemas de filmación o de escucha invada espacios reservados a la intimidad de las personas, aunque se haga desde emplazamientos alejados del recinto domiciliario, habrá de estar acordada en virtud de mandamiento judicial (instrumento habilitante para la intromisión en un derecho fundamental). Así, el material fotográfico y videográfico obtenido en las condiciones anteriormente mencionadas, y sin intromisión indebida en la intimidad familiar, tienen un innegable valor probatorio, siempre que sea reproducido en las sesiones del juicio oral correspondiente.

En relación con la filmación de ventanas de edificios desde los que sus moradores desarrollaban actividades delictivas, cuando es imprescindible para vencer obstáculos predispuestos para salvaguardar la intimidad, se ha estimado válida tal captación de imágenes siempre y

[663] Artículo 8.1 de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen: "No se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la Ley, ni cuando predomine un interés histórico, científico o cultural relevante".

cuando mediase una autorización judicial, no siendo sin embargo precisa para ver aquello que el titular de la vivienda no quiere ocultar a los demás[664].

Con arreglo pues a la doctrina jurisprudencial del Tribunal Supremo, toda filmación realizada por la policía, en una zona pública, donde se estén realizando actividades delictivas, no requiere autorización judicial previa y, no supondrá en ningún caso vulneración del derecho a la intimidad de las personas captadas por la grabación.

2.2.- Normativa en la UE.

En el marco comunitario no existe ninguna norma específica reguladora de las actividades de videovigilancia de las autoridades policiales por motivos de seguridad pública, de hecho, nada se dice sobre ello en Convenio 108 de 1981 del Consejo de Europa, aunque las actividades de vigilancia por videocámara que implican el tratamiento de datos personales entran en su ámbito de aplicación, dado que el Comité Consultivo (creado en virtud de este Convenio) estableció que las voces y la imagen se considerarán datos personales cuando aporten información sobre una persona y la hagan identificable, incluso indirectamente[665]. Por su parte, la Directiva 95/46/CE del Parlamento europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, excluye expresamente los tratamientos de datos en forma de sonido e imagen, como los que resultan de la vigilancia por videocámara: "cuando se aplican con fines de seguridad pública, defensa o Seguridad del Estado o para el ejercicio de las actividades del Estado relacionados con ámbitos del

[664] Sentencias del Tribunal Supremo nº 913/96 de 23 de noviembre, y nº 453/97 de 15 de abril.

[665] Comité Consultivo de la Convención, creado por el artículo 31 de la Directiva 95/46/CE, para la protección de las personas respecto al proceso automatizado de los datos de carácter personal. Destaca en cuanto a los riesgos del tratamiento de imágenes su "Informe de situación relativo a la aplicación de los principios de la Convención 108 a la recogida y al proceso de los datos biométricos". Estrasburgo, febrero de 2005.

derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario"[666].

Sin embargo, si se considera aplicable en el resto de casos, "considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos"[667].

El Grupo de Trabajo del Artículo 29 ha elaborado dos documentos orientativos sobre los riesgos de un uso abusivo de los sistemas de videovigilancia en relación con la protección de datos personales, y ha señalado las recomendaciones más pertinentes para evitarlos[668]. Este Grupo estima que el efecto psicológico que se produce, en relación con la vigilancia por videocámara, provoca que la opinión pública a veces considere este tipo de vigilancia, con o sin razón, una "herramienta inestimable" para la detección de delitos, lo que conlleva que se amplíe el margen de su utilización, produciéndose muchas arbitrariedades e intromisiones ilegítimas en los derechos fundamentales de las personas.

En los dos documentos, se parte de la base de que los datos relativos a personas físicas identificadas o identificables, constituidos por imagen y sonido, son datos personales:

---

[666] Considerando nº 16 de la Directiva 95/46/CE: "Considerando que los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario".

[667] Considerando nº 14 de la Directiva 95/46/CE.

[668] Se trata del Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara, Grupo del artículo 29 sobre protección de datos, de 11 de febrero 2004. Disponible en: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm [21 agosto, 2009] y, del Documento de trabajo relativo al tratamiento de datos personales mediante vigilancia por videocámara de 2002, ya citado.

"a) incluso si las imágenes se utilizan en el marco de un sistema de circuito cerrado y aunque no estén asociadas a los datos personales del interesado;

b) incluso si no se refieren a personas cuyos rostros hayan sido filmados, aunque contengan otra información, como, por ejemplo, números de matrícula o números de identificación personal (PIN) captados durante la vigilancia de cajeros automáticos;

c) independientemente del método utilizado para el tratamiento (por ejemplo, sistemas de vídeo fijos o móviles, como receptores de imagen portátiles, o imágenes en color o en blanco y negro), la técnica (dispositivos de cable o fibra óptica), el tipo de equipo (fijo, móvil o portátil), las características de la captación de imágenes (es decir, continua por oposición a discontinua, lo que ocurre, por ejemplo, cuando la captación de la imagen sólo se realiza en caso de que no se respete el límite de velocidad y no tiene nada que ver con la grabación de imágenes realizada de manera totalmente fortuita y poco sistemática) y las herramientas de comunicación utilizadas (por ejemplo, la conexión con un "centro" o el envío de imágenes a terminales remotos)".

En función de estos criterios, los Estados miembros verificarán si la vigilancia por videocámara implica el tratamiento de datos personales relacionados con personas identificables y, en ese caso, considera el Grupo de Trabajo, la Directiva 95/46/CE será aplicable independientemente de las disposiciones nacionales en las que se requiera además, autorización por motivos de seguridad pública.

En general, el Grupo de Trabajo del Artículo 29, entiende que "conviene que las instituciones pertinentes de los Estados miembros evalúen la vigilancia por videocámara desde un punto de vista general y con vistas a

impulsar un enfoque globalmente selectivo, además de sistemático, para este asunto. La proliferación excesiva de sistemas de captación de imagen en zonas públicas y privadas no deberá traducirse en la imposición de restricciones injustificadas a los derechos y libertades fundamentales de los ciudadanos; de lo contrario, los ciudadanos podrían verse obligados a someterse a procedimientos desproporcionados de recogida de datos que permitirían su identificación masiva en diversos lugares públicos y privados". Debe evitarse que el desarrollo de aplicaciones informáticas, basadas tanto en el reconocimiento fisonómico como en el estudio y el pronóstico del comportamiento humano, conduzca de manera involuntaria a una vigilancia preventiva. "Esta nueva forma de vigilancia está basada en la captación automatizada de los rasgos faciales de personas físicas y de su conducta "anormal", asociada a la disponibilidad de señales y avisos automatizados", lo que probablemente pueda acarrear incluso riesgos de discriminación.

En algunos casos la utilización de un sistema de grabación de imagen puede ser obligatoria, de conformidad con disposiciones específicas de los Estados miembros (por ejemplo, en casinos), o necesaria por cuanto se realiza con un fin al que los familiares de los afectados conceden especial importancia (por ejemplo, para la búsqueda de personas desaparecidas). Por otra parte también se pueden citar ejemplos peculiares del uso de tales dispositivos (en particular, relativos a terceros países), como aquellos casos en los que se han utilizado sistemas de reconocimiento fisonómico para impedir la bigamia o en los que una autoridad policial local ha decidido hacer públicas imágenes relativas a lo dura que es la vida en prisión para los presos, sin su consentimiento.

En general, se puede decir que si bien la vigilancia por videocámara parece estar en cierto modo justificada en determinadas circunstancias, también se dan casos en los que se recurre a la protección mediante videocámaras de manera impulsiva, sin considerar adecuadamente los requisitos y medidas pertinentes. En este sentido, se expresa el primer objetivo de los referidos documentos del Grupo de Trabajo de Artículo 29, diciendo que ha sido "atraer la atención hacia la amplia gama de criterios que existen para evaluar la legalidad y la conveniencia de instalar sistemas

individuales de vigilancia por videocámara", y para ello acude incluso a principios aparentemente lejanos como el de la protección del derecho a la libre circulación de las personas que se encuentran en el territorio de un Estado de manera legal[669], al señalar que:

> "Dicha libertad de circulación sólo puede estar sujeta a restricciones necesarias en una sociedad democrática, y proporcionales a la consecución de fines específicos. Los interesados tienen derecho a ejercer su derecho a la libre circulación sin verse sometidos a un condicionamiento psicológico excesivo en cuanto a sus movimientos y su conducta y sin ser objeto de un control detallado, como la posibilidad de que se sigan sus movimientos o se disparen "alarmas" basadas en programas informáticos que "interpretan" de manera automática la conducta supuestamente sospechosa de un individuo, sin ningún tipo de intervención humana, a causa de la utilización desproporcionada de la vigilancia por videocámara por parte de varias entidades en diversos lugares públicos o abiertos al público".

Opina el Grupo de Trabajo del Artículo 29 que la vigilancia por videocámara, realizada por motivos de necesidad reales de seguridad pública, o para la detección, prevención y control de delitos, debe en todo caso cumplir con los requisitos establecidos en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales y, en cualquier caso, estar cubierta por disposiciones nacionales específicas accesibles al público. La normativa que los Estados prevean al efecto, "debe estar relacionada con la prevención de riesgos concretos y delitos específicos y ser proporcional a éstos (por ejemplo, en locales expuestos a tales riesgos o en relación con acontecimientos públicos los cuales es razonablemente posible que den lugar a tales delitos)". Deberán tenerse en cuenta además otros efectos que producen los sistemas

[669] Artículo 2 del Protocolo Adicional nº 4 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

de vigilancia por videocámara, como el desplazamiento de las actividades vigiladas a otros lugares y, en cualquier caso, deberá especificarse siempre claramente "quién es el responsable del tratamiento, a fin de que los interesados puedan ejercer sus derechos. Éste último requisito también tiene que ver con el hecho de que cada vez es más frecuente que la vigilancia por videocámara la realicen conjuntamente la policía y otras autoridades públicas (por ejemplo, autoridades locales) o entidades privadas (bancos, asociaciones deportivas, empresas de transporte, etc.), lo que conlleva un riesgo de confusión en cuanto al papel y la responsabilidad individuales en relación con las tareas que se van a realizar".

Por último, además de aludir al principio de proporcionalidad, al derecho de información de los ciudadanos, al especial "derecho del interesado al olvido", a la brevedad del período de retención de las imágenes, y a la responsabilidad de los custodios de las imágenes, el Grupo de Trabajo del Artículo 29 se refiere expresamente a situaciones en que se recogen imágenes relativas a personas identificadas o identificables y que, de darse, requerirán de una evaluación caso por caso en los Estados en que se produzcan. Señala como más destacados los siguientes supuestos:

> a) Cuando existe una interconexión permanente entre sistemas de vigilancia de diferentes responsables del tratamiento.
>
> b) Cuando se permite la asociación de imágenes y datos biométricos (por ejemplo, en la entrada de bancos).
>
> c) "Utilización de sistemas de identificación vocal".
>
> d) Cuando se utilizan "sistemas de indexación relativos a imágenes grabadas o sistemas de recuperación simultánea automática, en particular a través de datos de identificación".
>
> e) Cuando se utilizan "sistemas de reconocimiento fisonómico que no se limiten a la identificación de camuflajes de

personas de paso, como barbas y pelucas falsas, sino que se basen en la localización de presuntos delincuentes, es decir, en la capacidad del sistema para identificar automáticamente a determinados individuos: A partir de plantillas o retratos robot que resulten de determinados rasgos externos (como el color de la piel o los ojos, la prominencia de los pómulos, etc.) o con arreglo a comportamientos anormales predefinidos (movimientos repentinos, paso por el mismo lugar incluso a intervalos determinados, manera de aparcar un vehículo, etc.)".

f) Cuando se permite localizar automáticamente itinerarios y pistas, o reconstruir o prever el comportamiento de una persona.

g) Toma de decisiones automatizadas basadas en el perfil de una persona o en análisis inteligentes y sistemas de intervención que no estén relacionados con señales de alarma estándar (como el hecho de entrar en un lugar sin la identificación necesaria o una alarma de incendio).

Por último, en otros supuestos concretos del uso de cámaras de videovigilancia para la protección de la seguridad pública y, respecto de los riesgos que ello conlleva para la intimidad de los afectados, se quiere llamar la atención sobre el Asunto Perry contra el Reino Unido, sentenciado con fecha 17 de Julio de 2003, por el Tribunal Europeo de Derechos Humanos, realizando un análisis detallado de la resolución dictada. El asunto tiene su origen en una demanda de un ciudadano británico (Stephen Arthur Perry) contra el Reino Unido, presentada ante el Tribunal (el 06-10-2000), por la grabación y uso para identificación en rueda de reconocimiento de imágenes de vídeo tomadas en comisaría de policía sin el consentimiento del demandante y posterior uso en juicio. El demandante se queja, en virtud del artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de que la Policía le grabó de manera encubierta de cara a identificarle y utilizó el material en la acusación contra él.

En el caso enjuiciado, el demandante era un ladrón habitual que fue detenido en varias ocasiones, pero que, aun aceptando ser sometido a rueda de reconocimiento, en las últimas ocasiones no se había presentado a tal efecto ante las autoridades policiales. Por este motivo, y por ser esto de gran importancia para el caso (robos a mano armada, sucedidos en septiembre y octubre de 1997), la Policía decidió organizar una rueda de identificación en vídeo. Se solicitó permiso al Subjefe de la Policía para grabar encubiertamente en vídeo al demandante de acuerdo con las Directrices del Ministerio del Interior para el uso de aparatos en las operaciones de vigilancia policial de 1984.

El 19 de noviembre de 1997, el demandante fue llevado de la prisión (en la que estaba interno por otro asunto), a la Comisaría de Policía. La prisión y el demandante habían sido informados de que el motivo del traslado era la identificación e interrogatorio referente a los robos a mano armada. Al llegar a la Comisaría de Policía se le pidió que participara en la rueda de identificación, y éste se negó.

Mientas tanto, a su llegada a la Comisaría de Policía, fue filmado por el sistema de cámara de la zona de seguridad que se mantiene en funcionamiento en todo momento y que está situada en una zona por la que van y vienen el personal de la Policía y los sospechosos. Un ingeniero había ajustado la cámara para garantizar que tomara imágenes claras durante su visita, y fuera posible someter las imágenes a reconocimiento por los testigos del caso, tal y como después se hizo, resultando identificado por dos de ellos. Ni el demandante ni su abogado fueron informados de que se había preparado una cinta o de que ésta se había utilizado para una rueda de reconocimiento, ni se les dio la oportunidad de visionarla antes de que fuera utilizada.

Comenzado el primer juicio, el Juez admitió el vídeo como prueba, aun reconociendo que no se había ajustado Código de Práctica (anexo a la Ley de Pruebas Penales y Policiales de 1984), entre otras cosas, por no haber solicitado el consentimiento del demandante para la grabación del vídeo, por no haberle informado de su existencia, no haberle informado de

su uso en una rueda de identificación y tampoco de sus derechos a este respecto (esto es, darle la oportunidad de ver el vídeo, de plantear objeciones sobre su contenido e informarle del derecho de su abogado a estar presente cuando los testigos visionaran la cinta de vídeo). El Juez decidió que no había ninguna ilegalidad en el uso de la cinta de vídeo y fue mostrado al Tribunal que tuvo la oportunidad de ver exactamente cómo se había desarrollado todo el proceso de identificación. Finalmente, el demandante fue declarado culpable por el jurado, y decidió recurrir la Sentencia. El Tribunal de Apelación desestimó el recurso, y acudió a la Cámara de los Lores, que no pudieron resolver porque en Apelación esta posibilidad le había sido negada.

La normativa nacional que en este caso era aplicable, además del Artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950)[670], se limitaba a una serie de Directrices del Ministerio del Interior del Reino Unido, y la Ley de Pruebas Penales y Policiales de 1984 (PACE), junto con su Código de Práctica anexo.

Las Directrices del Ministerio del Interior especificaban que únicamente los Jefes de Policía o Asistentes de los Jefes de Policía tenían competencias para conceder autorizaciones para el uso de esos dispositivos, en función de una serie de requisitos específicos:

- que la investigación se refiriese a un delito grave;

- que se hubieran intentado métodos de investigación normales y que hubieran fracasado, o que se desprenda de la naturaleza de las cosas, que sería improbable que tuvieran éxito si se intentasen;

[670] Artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950):
"1. Toda persona tiene derecho al respeto de su vida privada (…)
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la Ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

- que hubiera una buena razón para pensar que el uso del equipo lleve a una detención o a una condena, o cuando sea apropiado, a prevenir actos de terrorismo;

- que el uso del equipo fuera factible operativamente;

- que el grado de intrusión en la intimidad de las personas afectadas por la vigilancia fuese en todo caso proporcionado a la gravedad del delito.

Por su parte, la Ley de Pruebas Penales y Policiales de 1984, en su artículo 78, disponía que un Tribunal podría negarse a admitir pruebas, si teniendo en cuenta todas las circunstancias (incluidas aquellas en las que dichas pruebas fueron obtenidas), se verificase que "su admisión tendría un efecto tan negativo en la equidad del procedimiento que el Tribunal no debiera admitirlas"[671]. Y el Código de Práctica señalaba, en lo relativo a la práctica de la prueba de identificación del sospechoso, que la autoridad policial tiene cierta libertad:

a) "La Policía podrá realizar ruedas diferentes de una rueda de identificación si el sospechoso se niega o si, habiendo estado de acuerdo, no se presenta a la rueda de identificación.

b) El agente de identificación podrá mostrar a los testigos un vídeo del sospechoso si el agente considera, bien a causa de la negativa del sospechoso a participar en una rueda o un grupo de identificación, bien por otras razones, que eso será, en las circunstancias del caso, la línea de conducta más satisfactoria.

c) Se informará al sospechoso (en nota escrita, para ser firmada por él y de palabra) de la finalidad de la rueda o el

[671] En el caso R. contra Khan (1996), una prueba obtenida colocando un dispositivo de escucha en una casa privada sin el conocimiento de sus ocupantes, en violación del artículo 8 del Convenio, fue admitida, confirmando la discrecionalidad del juez ante estas situaciones.

vídeo de identificación y el procedimiento para celebrarlo (personas que pueden estar presentes para apoyarle), y si aún así no consiente en participar, su negativa puede ser presentada como prueba en un juicio posterior y la Policía puede proceder de manera encubierta sin su consentimiento o puede establecer otras disposiciones para comprobar si un testigo le identifica".

Partiendo de esta base normativa, se analizaron los alegatos de las partes.

El demandante consideraba que ser filmado en la Comisaría de Policía había violado su derecho al respeto de su vida privada. Negó ser consciente de estar siendo grabado para fines de identificación (es más, la cámara le había grabado a diferente velocidad para producir una imagen más nítida y clara del demandante) y, alegó que no puede considerarse que la PACE autorice la recogida de imágenes sin el conocimiento del sospechoso cuando no se han seguido las normas.

El Gobierno del Reino Unido consideró por su parte que la grabación no se había hecho en un lugar privado, sino que se había llevado a cabo en la zona de seguridad de la comisaría, que es una zona común administrativa por la que tienen que pasar todos los sospechosos y en la que funciona, por rutina, un circuito cerrado de vídeo que es fácilmente visible. Las imágenes eran por tanto públicas, no privadas y, el demandante no podía razonablemente esperar intimidad en tal entorno y había sido informado que estaba allí para identificación. Además, las imágenes no fueron tomadas con fines de vigilancia, sino con fines de identificación, y únicamente para su uso en el procedimiento penal[672]. El uso de las imágenes fue similar al uso que se hace de las fotografías en los álbumes de identificación de la autoridad policial[673].

[672] Se justificaba este argumento en los asuntos Friedl contra Austria (Informe de la Comisión de 19 mayo 1994) y Lupker y otros contra Holanda (Informe de la Comisión de 7 diciembre 1992).
[673] Esta circunstancia, en teoría no planteaba conflicto, sobre todo cuando son utilizadas únicamente con fines de identificación de delincuentes en un procedimiento penal (Lupker y otros contra Holanda).

El Gobierno entendía que tampoco se puede decir que la imágenes fueran "procesadas", ya que la imagen de la parte del demandante fue simplemente extraída y colocada junto con las imágenes de once voluntarios de la rueda de reconocimiento y las imágenes no se difundieron o emitieron en público.

La base legal que utilizó para justificar dichas actuaciones, fue el Código de Práctica de la PACE, porque dispone un procedimiento de identificación por vídeo y la recogida de imágenes sin el conocimiento del sospechoso, si el sospechoso no consiente en participar en una rueda de identificación.

La injerencia pues perseguía el fin legítimo de la protección de la seguridad pública, la prevención del delito y la protección de los derechos y las libertades de los demás y, ya que el demandante no se había presentado o se había negado a participar en ruedas de identificación, se podía considerar razonablemente que era una medida "necesaria en una sociedad democrática".

Finalmente el Tribunal Europeo de Derechos Humanos resolvió a favor del demandante, y su justificación merece ser analizada. El Tribunal consideró que era necesario delimitar el término "vida privada". Existe una zona de interacción de una persona con las otras, incluso en un contexto público, que puede entrar en el ámbito de "vida privada" y por lo tanto, la ésta puede verse afectada por medidas llevadas a cabo de fuera de la casa de esa persona o de lugares privados en sentido estricto[674]. También estableció que la grabación de datos y la sistemática o permanente naturaleza de una grabación por los servicios de seguridad, incluso sin el uso de métodos de vigilancia encubierta, puede plantear una injerencia en la vida privada de los demandantes, considerándose como registro o recogida

[674] En el caso P. G. y J. H. contra el Reino Unido (2001), la grabación permanente de las voces de P. G. y J. H. fue hecha mientras respondían a preguntas en una zona pública de la comisaría de Policía cuando agentes de Policía les estaban interrogando, la grabación de sus voces para un posterior análisis se consideró como el registro de datos personales sobre ellos, lo que supuso una injerencia en su derecho al respeto de sus vidas privadas. En Peck contra el Reino Unido (Sentencia de 28 enero 2003), la difusión a los medios de comunicación para su emisión de imágenes de vídeo del demandante cuyo intento de suicidio fue captado por un circuito cerrado de cámaras de televisión, fue considerado como una grave injerencia en la vida privada del demandante, a pesar de que se encontraba en ese momento en un lugar público.

de datos personales sobre el demandante[675]. El uso normal de cámaras de seguridad, bien en las calles bien en lugares públicos como centros comerciales o comisarías de Policía, cuando sirven a un fin legítimo y previsible, no plantea por si mismo ninguna cuestión en virtud del artículo 8.1 del Convenio, sin embargo, lo cierto es que la Policía reguló la cámara de seguridad para que pudiera tomar imágenes nítidas del demandante en la zona de seguridad, imágenes que fueron insertadas en un montaje con otras personas que les fue mostrado a los testigos para ver si podían identificar al demandante como el autor material de los robos que se estaban investigando.

Por otra parte, la publicación del material en grado y manera superiores de lo normalmente previsible puede hacer también entrar a las grabaciones de seguridad en el ámbito del artículo 8.1. del Convenio. El vídeo fue mostrado durante el juicio del demandante en una sala de tribunal abierta al público. Y la utilización de fotografías en los álbumes de identificación, no puede considerarse como análogo a este caso, pues las fotografías no llegan a manos de la Policía mediante una invasión de la intimidad, sino que habían sido aportadas voluntariamente a las autoridades para las solicitudes de pasaportes o habían sido tomadas por la Policía con ocasión de un arresto anterior. Las imágenes en cuestión en este caso no fueron obtenidas voluntariamente o en circunstancias en las que se pudiera razonablemente prever que serían grabadas y utilizadas para fines de identificación.

Finalmente, el Tribunal consideró que la grabación y el uso de las imágenes de vídeo del demandante en este caso supone una injerencia en su derecho al respeto de su vida privada, pero se plantea si tal injerencia era o no justificada, principalmente, si estaba "prevista por la Ley". Consideró que la grabación y el uso de imágenes de vídeo para identificación tenía una base suficiente en la legislación interna y tenía la calidad exigida para satisfacer los dos requisitos indicados, pero en este caso, la Policía no había cumplido con el procedimiento establecido en el Código aplicable en al

[675] Asuntos Rotaru contra Rumania, de 4 de mayo de 2000 (Sentencia 130/2000), y Amman contra Suiza, de 16 de febrero de 2000 (Sentencia 87/2000). TEDH.

menos tres aspectos: no solicitaron al demandante su consentimiento para el vídeo, en no informarle de su existencia y uso para identificación y en no informarle de sus propios derechos a ese respecto (esto es, a darle la oportunidad de visionar el vídeo, poner objeciones a su contenido e informarle del derecho de su abogado a estar presente cuando los testigos visionaran la cinta de vídeo), y por lo tanto, no se ha cumplido con la legislación interna. En este aspecto, el Tribunal consideró que la injerencia no estaba "prevista por la Ley" como exige el segundo apartado del artículo 8 y que hubo una violación de esta disposición.

3.- Bases de datos genéticas.

En el mes de Junio de 2006, el que era el Ministro del Interior, D. Alfredo Pérez Rubalcaba, señalaba en una comparecencia ante el Senado "que los avances en la construcción y consolidación de un verdadero espacio de libertad, de seguridad y de justicia en Europa son continuos (…) se consolidan grupos de cooperación reforzada en materia de seguridad, tales como el G-6 o el que constituyen los países del llamado Tratado de Prum, a los que España pertenece y en los que participamos activamente".

El Tratado de Prum[676] fue suscrito por España en el año 2005, y permite la transferencia internacional de datos policiales, incluidos pruebas de ADN y huellas dactilares.

Este documento es considerado como un instrumento fundamental para la cooperación entre autoridades policiales, principalmente dentro del grupo de Schengen y, se basa en las posibilidades técnicas que existen hoy para "inventariar" colectivos humanos. No cabe duda de que nuestro modelo

[676] Tratado de Prum, entre el Reino de Bélgica, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la república de Austria, relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal. (2005).

de Estado necesita gestionar de la forma más eficiente enormes cantidades de datos de carácter personal, pero como ya se ha señalado no es menos cierto que la gestión de esta información debe estar siempre delimitada bajo unos mínimos parámetros de constitucionalidad, es decir, con total respeto a los derechos fundamentales de quienes quedan a disposición del Estado y quienes en definitiva se pretende proteger. Un tratamiento de datos de carácter personal sin garantías de confidencialidad o, sin límites a la finalidad de su tratamiento, puede afectar a todos los aspectos de la vida de una persona, por tanto, en función de cuál sea el más vulnerable, habrán de determinarse mayores o más específicas precauciones.

El material genético de un individuo, su perfil de ADN, es si cabe el dato de carácter personal más sensible que existe; describe tanto el conjunto de la información biológica hereditaria de una familia, como cada elemento identificador físico personal de cada individuo, único e irrepetible. La correcta protección de los datos genéticos puede considerarse hoy como una condición previa para "garantizar el respeto del principio de igualdad condición previa para garantizar el respeto del principio de igualdad y para que el derecho a la salud exista realmente. Todos los instrumentos internacionales recientemente publicados prohíben de hecho cualquier discriminación basada en datos genéticos. Según el artículo 21 de la Carta de los derechos fundamentales de la UE, está prohibida "toda discriminación (…) ejercida por razón de (…) características genéticas", y esta prohibición se encuentra en el Convenio sobre los Derechos Humanos y la Biomedicina (artículo 11) y en la Declaración Universal sobre el Genoma Humano y los Derechos Humanos de la UNESCO (artículo 6)"[677].

Toda esta información es un instrumento de enorme valía para un Estado, pues le permite cumplir eficientemente con muchas de sus funciones, como la averiguación de los delitos o la identificación de los delincuentes. Poder disponer de dicha información con cierta flexibilidad es un objetivo que debe ser aceptado con cautela, sobre todo, por cuanto debe ser regulado con absoluto respeto a los derechos humanos. Si la meta es

[677] Grupo de Trabajo del Artículo 29. Documento de trabajo sobre datos genéticos, adoptado el 17 de marzo de 2004. p.2.
Disponible en: www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp91_es.pdf

proteger los derechos individuales de las vulneraciones más graves, difícilmente se podrá lograr si se ignoran las garantías que conforman su esencia y eficacia. En este sentido, se ha promulgado con fecha 8 de octubre de 2007, la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, que más adelante se analizará.

3.1.- Posibilidades de tratamiento para las autoridades policiales.

La instrumentalización del ADN consiste en procesar científicamente el código genético y, en archivarlo estructuradamente, de tal forma que permita localizar e identificar con rapidez al titular de la muestra estudiada. El ámbito en el que esta instrumentalización ha tenido prioridad hasta ahora es en el ámbito de la asistencia sanitaria y por ello, los textos normativos más importantes que existen sobre esta materia, han sido dictados en relación con el tratamiento sanitario de datos genéticos: la Declaración Universal sobre el Genoma Humano y los Derechos Humanos (1997) y, el Convenio para la Protección de los Derechos Humanos de Oviedo[678]. Ambos documentos ponen de manifiesto el principio fundamental de que los tratamientos de datos genéticos realizados fuera del ámbito sanitario, deben ser limitados siempre a lo necesariamente imprescindible. Por lo tanto, cuando nos encontremos en el ámbito de una investigación policial, debe considerarse en primer lugar que el conocimiento de datos genéticos va a afectar indiscutiblemente al ejercicio de la libertad personal y, que debe ser limitado al máximo.

[678] Declaración Universal sobre el Genoma Humano y los Derechos Humanos aprobada en la Conferencia General de la UNESCO, el 11 de noviembre de 1997, y el Convenio para la Protección de los Derechos Humanos y la Dignidad del Ser Humano con respecto a las aplicaciones de la biología y la medicina, firmado en Oviedo el 4 de abril de 1997, ratificado por España en 1999.

La Resolución del Parlamento Europeo, de 16 de marzo de 1989, sobre los problemas éticos y jurídicos de la manipulación genética, dispone que "los análisis genéticos en los procedimientos judiciales sólo pueden realizarse con carácter excepcional y exclusivamente por orden judicial y en ámbitos estrechamente delimitados y que se puedan utilizar únicamente aquellas partes del análisis del genoma que revisten importancia para el caso y que no permitan ningún tipo de deducciones sobre la totalidad de la información hereditaria". Es decir, se limita la utilización del material desde su finalidad (fines policiales) y, por su composición (material no codificante).

Por otra parte, la Recomendación 92 (1) del Comité de Ministros del Consejo de Europa[679], se refiere a la posibilidad de creación de estas bases de datos en los artículos 8 a 11, y remite a los Estados miembros para su regulación. Esta Recomendación aceptaba a posibilidad de archivo de información genética sobre reos de delitos sexuales u otros de similar gravedad contra la integridad de las personas, pero no distingue entre el material codificante y el material no codificante, por lo que ha de entenderse que su aplicación final deberán especificarla los Estados miembros en la regulación y norma especial que quieran darle.

En las regulaciones estatales ha de tenerse en cuenta que los elementos científicos y tecnológicos disponibles para realizar los análisis genético, son los que van a marcar el ritmo de los elementos jurídicos de sus límites ya que, si bien es cierto que hoy un análisis de laboratorio puede darnos por una parte ADN codificante (expresivo), que aporta la información genética sobre la configuración del individuo y, por otra parte, ADN no codificante, información de características físicas individuales, no lo es menos que desconocemos las posibilidades de tratamiento que nos ofrecerá en un futuro (por ejemplo, respecto de la clonación), y de ahí la importancia de esclarecer los límites al uso o manipulaciones de uno y otro código.

En un eventual tratamiento de datos genéticos para su almacenamiento en bases de datos policiales, el primer punto a tener en

[679] La Recomendación 92 (1) del Comité de Ministros del Consejo de Europa, de 10 de febrero de 1992, sobre uso de los análisis de ácido desoxirribonucléico – ADN- dentro del marco del sistema judicial penal.

cuenta será ver si se trata de ADN no codificante, que es el que va a permitir identificar a la persona afectada como única, mostrando su "huella genética" sin aportar otros datos más sensibles, como por ejemplo, los que afecten directamente a su salud. Este ha de ser por tanto el material definitorio, esencial para la configuración y límite jurídico de las bases de datos de ADN policiales, pues marca lo que es estrictamente necesario conocer en las investigaciones penales, para una identificación precisa de los individuos.

Por otra parte, el procedimiento científico a seguir también debe tenerse en cuenta para definir dichos elementos jurídicos, porque para realizar una prueba de ADN es necesario seguir un procedimiento concreto consistente en señalar el objeto del análisis, extraer las muestras y proceder a su estudio. Todo ello podría llevar a configurar hasta tres bases de datos distintas susceptibles de tratamiento, dependiendo de la información de carácter personal manipulada en cada fase. Una sería la base de datos configurada por la fuente de obtención de las muestras, pero dentro de ella, podría crearse otras bases de datos o clasificación distintas: de los condenados por un delito, de los sospechosos y/o de sus víctimas, de las víctimas de una catástrofe, de individuos anónimos que aportan sus muestras voluntariamente o cuyas muestras han sido recogidas de una escena del crimen, etc.

Toda esa información permite realizar estudios con un gran volumen de individuos implicados y, pueden ser utilizados para conocer de su predisposición a la violencia, como elemento hereditario; de la identidad de desaparecidos y asesinados en periodos dictatoriales; de los profesionales de las Fuerzas Armadas (su identificación) en caso de necesidad; estudios para evidenciar el parentesco biológico de los implicados en la comisión de un delito o en la investigación de desaparecidos; estudios para la investigación histórica, etc. En definitiva, son numerosas las posibilidades que ofrece la identificación genética, pero siempre se tendrán que ver limitadas por los elementos jurídicos de su definición legal, y en especial, por los principios de proporcionalidad y de calidad, pues de lo contrario, se presentaría un serio problema de constitucionalidad.

Los límites de creación de las bases de datos son una parte de su definición jurídica, pero otra parte esencial lo serán en todo caso los límites de su uso por las Fuerzas de Seguridad del Estado, de forma que efectivamente se preserve la dignidad personal de los individuos afectados. Cada posibilidad contará para determinar las pautas jurídicas del tratamiento datos genéticos, y más en el ámbito penal, donde es ya habitual y necesario practicar pruebas de identificación, averiguación y comprobación, tanto del delincuente como de la víctima, y donde existen consecuencias que podrían implicar la total desprotección de la persona.

El Tribunal Constitucional ha puesto de manifiesto la importancia de estos límites en su Sentencia de 16 de diciembre, 207/1996, donde señalaba que desde un principio, toda medida de intervención corporal afecta al derecho fundamental a la integridad física y, exigía la intervención del juez en el ámbito procesal penal. En una Sentencia anterior[680], el Tribunal Constitucional ya señalaba que la práctica del análisis de la huella genética significa una injerencia en los derechos fundamentales y que, por ello, es imprescindible la observación del principio de proporcionalidad. También desde Europa se ha afirmado en numerosas ocasiones (Comisión Europea de Derechos Humanos) que toda intervención corporal constituye una intromisión en el derecho al respeto de la vida privada protegido por el artículo 8 del Convenio Europeo de Derechos Humanos. Este precepto literalmente prevé que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia y además que no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". Sobre esta base, se ha ido perfilando la configuración de límites al tratamiento de la información genética en los distintos Estados miembros, conscientes de que la dignidad puede "desaparecer cuando el control estatal

[680] Sentencia del Tribunal Constitucional 37/1989, de 15 de Febrero de 1989, F.Jº. 7º: "en la que se hace referencia a la reiterada doctrina según la cual la regla de la proporcionalidad de los sacrificios es de observancia obligada al proceder a la limitación de un derecho fundamental".

alcanza tal cantidad de información de manera que los individuos se encuentran por completo "fichados" y esto evidencia que hay que lograr la satisfacción del interés público con la menor injerencia posible en los derechos fundamentales del individuo" [681].

En España, los ficheros con perfiles de ADN se tratan dentro del marco dispuesto por el artículo 18. 4 de la CE, y son considerados bases de datos de carácter personal, con la obligada protección que corresponde a este derecho fundamental aunque eso si, siempre con la necesaria proporcionalidad respecto de un derecho que, por otra parte, no es ilimitado.

Las garantías previstas constitucionalmente para la protección de los datos de carácter personal, son límites, y están establecidos para la protección del individuo, pero también es cierto que en tampoco deben suponer un obstáculo para el desarrollo de la actividad policial o de la actividad procesal penal, más allá de lo dispuesto por el siempre aplicable principio de proporcionalidad. Por este motivo, bajo determinadas circunstancias, se habrán de ponderar de la forma más flexible, tanto la necesidad de su tratamiento, como sus límites para la investigación penal. Por ejemplo la LOPD rompe, por su gravedad, con los límites mínimos del tratamiento de bases de datos genéticos cuando sean objeto de tratamiento para en la "lucha contra el terrorismo, contra formas graves de delincuencia organizada"[682]. Sin embargo, cuando se trata de las competencias ordinarias de investigación de las autoridades policiales, la Ley 15/1999 de Protección de Datos es aplicable en todos sus términos.

En España se permite el tratamiento de dos tipos de ficheros de perfiles de ADN: los que contienen datos personales de delincuentes (forenses criminales) y, los que contienen datos personales de personas desaparecidas (forenses civiles).

[681] TRONCOSO REIGADA, A. "Estudios sobre Administraciones Públicas y protección de datos personales", I Encuentro entre Agencias Autonómicas de Protección de Datos Personales. Ed. APDCM. Distribución Civitas Ediciones S.L. 2006. p.36 y 37.
[682] Artículo 2.2.c) de la Ley 15/1999 de Protección de Datos de Carácter Personal.

Entre la Guardia Civil y la Policía Nacional se reparten distintos programas de tratamiento, de los que cabe destacar para los primeros el Programa Fénix de Identificación Genética de personas desaparecidas (1997) o, la base de datos ADNIC, destinada a "cooperar con la Administración de Justicia mediante la identificación genética de vestigios biológicos y la identificación genética de vestigios biológicos y la identificación genética de muestras de origen conocido en usos de investigación policial"[683] (delincuentes) y, para los segundos, el "Programa Genio" (2000) compuesto por dos bases de datos, "Veritas", destinada a "colaborar con la Administración de Justicia en la represión de infracciones penales con identificación genética de vestigios biológicos recogidos en la investigación de presuntos delitos o muestras de la misma naturaleza a solicitud de la autoridad competente"[684] (desaparecidos) y, "Humanitas", destinada a la "identificación de restos humanos de víctimas de hechos catastróficos o criminales y cadáveres de desaparecidos por ADN extraído de los mismos, e investigaciones del Cuerpo Nacional de Policía con los citados fines"[685] (delitos).

Constan también declarados ante la AEPD otros ficheros similares, aunque con finalidades puramente científicas. El llamado "Fichero del Banco Nacional de ADN", de la Universidad de Salamanca, tiene asignada, como finalidad exclusiva, la selección de muestras para estudios de investigación genética sobre la evolución humana, los genes que influyen en el desarrollo de determinadas enfermedades, la influencia del entorno del individuo en las mismas y los genes que influyen en la eficacia de determinados tratamientos específicos, o también, el perteneciente al Instituto Nacional de Toxicología y Ciencias Forenses, que se denomina "Muestras y Resultados" y que se destina a la gestión de las muestras analizadas (custodia) y de los datos obtenidos en los análisis realizados con fin investigador.

En el ámbito europeo, los países que aceptan el tratamiento de datos genéticos a día de hoy son: Croacia, Francia, Inglaterra, República

[683] Descripción del fichero en su Registro ante la AEPD. www.agpd.es.
[684] Ibidem.
[685] Ibídem.

Checa, Bélgica, Inglaterra, Irlanda del Norte, Escocia, Estonia, Holanda, Austria, Eslovaquia, Alemania, Hungría, Suiza, Suecia, Eslovenia, Finlandia, Letonia, Noruega, Dinamarca, Polonia, Portugal, España, Grecia y Yugoslavia. Las experiencias de colaboración habidas entre los Estados de la UE han dado resultados muy positivos en la identificación de personas, tanto de desaparecidos como de delincuentes o, de sus víctimas. Cabe destacar el programa de identificación de ADN llevado a cabo por el grupo de trabajo International Commission on Missing Persons (ICMP), creado en 1996 para la identificación de las víctimas de las guerras de Croacia, Bosnia Herzegovina, Kosovo, Macedonia, y de la antigua Yugoslavia. Junto a éste, realizan también identificaciones de carácter genético, el Grupo Español y Portugués de la Sociedad Internacional de Genética Forense (GEPISFG)[686] y, el Grupo de Trabajo en ADN (DNA Working Group) de la Red Europea de Institutos Forenses (European Network of Forensic Science Institutes (ENFSI)[687]. En esta línea de trabajo, es necesario citar también al grupo de de colaboración formado entre miembros de la Comisaría General de Policía Científica y, del Instituto Nacional de Toxicología y Ciencias Forenses, creado en España especialmente para la investigación del atentado del 11-M, tanto para la identificación de las víctimas como de los terroristas, y su homólogo anterior, creado para la identificación de las víctimas de los ataques terroristas del 11 - S al World Trade Center de la ciudad de Nueva York, en el que se han analizado más de 26.000 restos humanos en el programa MFISYs (Mass Fatalyty Incident System, desarrollado por GeneCodes Corporation).

[686] http://www.ertzaintza.net/adn_nuclear
[687] www.str-base.org

3.2.- Regulación normativa y criterios de la AEPD.

Las dudas e incógnitas que más frecuentemente ofrece la regulación normativa de este tipo de bases de datos y ficheros de datos de carácter personal, son por norma las relativas al tipo de tratamiento que permiten y, al riesgo de vulneración de los derechos a la protección de datos personales, e incluso al derecho a la intimidad, es decir, a la ponderación de riesgos. Los órganos legislativos se plantean cuestiones tales como ¿quién puede ser incluido un perfil de ADN en la base de datos?, ¿en qué momento? o, ¿cuánto tiempo se puede conservar esa información?, y en función de las respuestas que se den y, de la flexibilidad de actuación que permitan, se configurará su regulación específica como sistema de análisis de la población y de conservación de muestras, es decir, bien como el conjunto de muestras específicamente tomadas para investigaciones de carácter policial especiales (violaciones, desaparecidos, asesinatos, terrorismo, etc.), o bien, como análisis genético de un caso concreto, tanto para el sospechoso, como sobre los vestigios recogidos específicamente para la investigación de tal hecho.

El equilibrio para elaborar una normativa sobre estos instrumentos de investigación que, por definición ponen en peligro derechos fundamentales, ha venido condicionado no sólo por el respeto a lo dispuesto en la Constitución sobre la obligatoria reserva de Ley, sino también por lo dispuesto en la normativa europea en materia de derechos humanos, y en el caso que nos ocupa, ha de estarse en primer lugar al Convenio Europeo de Derechos Humanos. Sobre una eventual restricción del derecho a la vida privada, dicho Convenio recoge el deber de respeto de intimidad y de los datos de carácter personal, siempre y cuando estas medidas estén previstas por la Ley[688] concreta[689], que en nuestro ordenamiento no es otra que el

[688] Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, de 4 de noviembre de 1950, ratificado por España con fecha 26 de septiembre de 1979, y publicado en el Boletín Oficial del Estado de 10 de octubre de 1979.
Artículo 8. Derecho al respeto a la vida privada y familiar.
1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

instrumento "Ley Orgánica", específico para el desarrollo de los derechos fundamentales y de las libertades públicas y, que exige para su aprobación, modificación o derogación, la votación final favorable sobre el conjunto del texto, por mayoría absoluta del Congreso.

Los intentos de regular el tratamiento de los perfiles de ADN de forma conjunta, comenzaron con una Proposición de Ley de febrero 1995 y después, con un Anteproyecto de Ley de mayo de 1998. En 1995, el Partido Popular presentó ante el Congreso de los Diputados, una Proposición de Ley denominada "Uso y práctica del análisis del ADN dentro del sistema del derecho penal y en la investigación de la paternidad". Se trataba de un breve texto, de nueve artículos que quería regular todas las cuestiones relacionadas con las intervenciones corporales, los análisis genéticos y, con la conservación y posterior almacenamiento de la información genética. Paralelamente, el Gobierno de aquel momento, promulgaba la Orden Ministerial de 26 de julio de 1994 para regular la creación y gestión de determinados ficheros con datos de carácter personal, que serían gestionados por el Ministerio del Interior. Entre estos ficheros, se incluía un fichero de perfiles de ADN bajo la responsabilidad de la Dirección General de la Policía, que almacenaría las "bandas de ADN de las personas implicadas en la comisión de hechos delictivos" y tendría como finalidad "la identificación de implicados en delitos mediante bandas de ADN". Esta Orden trataba de adecuar estos tratamientos a la LORTAD (Ley Orgánica 5/92 de 29 de octubre) y, a ella le siguió la Orden de 18 de marzo de 1998 por la que se regulaba el fichero automatizado FENIX (de identificación genética de cadáveres/desaparecidos) y, la Orden de 7 de marzo de 2000, por la que se reguló el fichero ADNIC (de identificación genética de vestigios biológicos), ambos de la de la Dirección General de la Guardia Civil. Por otra parte, los ficheros ADN Humanitas y ADN Veritas del Cuerpo Nacional de Policía fueron creados con posterioridad, por una Orden de 21 de septiembre

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

[689] Tribunal Europeo de Derechos Humanos, Sentencia Malone de 2 de agosto de 1984, "el artículo8.2 del Convenio no se limita a remitirse al Derecho interno sino que se refiere a la calidad de la ley".

de 2000. Finalmente, la Orden del Ministerio del Interior de 20 de junio de 2002, adaptó su regulación a la LOPD[690] y, se culminó el proceso con la promulgación de la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

Esta situación normativa, además de estar basada en la Ley de Protección de Datos, estaba ya "encargada" por la Recomendación R (92) 1 del Comité de Ministros a los Estados miembros sobre la utilización de los análisis de ácido desoxirribonucleico (ADN), dentro del marco del sistema de justicia penal, que establecía que la obtención de muestras para realizar los análisis de ADN se efectuaría de conformidad al derecho interno y, que debía ser autorizado cualquiera que fuese el nivel de gravedad de la infracción pero, siempre bajo la finalidad exclusiva de la investigación y persecución de hechos criminales. Así expuesto, el objeto de la norma hacía peligrar el principio de proporcionalidad, y por ello se quiso matizar explicando que si el estudio del ADN era solicitado por el imputado para su defensa, entonces podría ser ampliado el conjunto de delitos a ser investigados en ese entorno. Igualmente, respecto a su conservación ilimitada, la Recomendación establecía que podían ser conservados cuando el interesado hubiera sido reconocido culpable de delitos graves y, cuando éstos atentan contra la vida, la integridad o la seguridad de las personas. Estos criterios han sido adoptados por los Estados miembros de formas distintas, así Gran Bretaña permitía la conservación de perfiles de ADN por tiempo indefinido al no establecer límites con criterios punitivos, y al contrario, Alemania, por su pasado histórico de desaparecidos y persecuciones de sangre, puso mayor cuidado en la delimitación de estas prácticas, considerando sólo supuestos verdaderamente graves (delitos de violencia sexual y homicidios)[691].

[690] GUILLÉN VÁZQUEZ, Margarita. "Bases de datos de ADN con fines de investigación penal. Especial referencia al derecho comparado", Estudios Jurídicos (2004). Centro de estudios Jurídicos del Ministerio de Justicia. Disponible en: www.cej.justicia.es/pdf/publicaciones/fiscales/FISCAL40.pdf

[691] Sentencia de 1995 del Tribunal Constitucional alemán, para la cual la idea de una justicia penal eficaz exige la satisfacción del interés procesal en la investigación de la verdad. Además, sostiene que el esclarecimiento de los hechos punibles graves constituye una misión especial del Estado de Derecho, y hace presente que la práctica de la huella genética supone una injerencia en el ámbito de los derechos fundamentales que exige, por consiguiente, la observación del principio de proporcionalidad, el cual requiere que la medida sea indispensable y se encuentre en una relación proporcionada a la gravedad del hecho.

Sobre los antecedentes normativos señalados, la Agencia Española de Protección de Datos (AEPD) ha tratado de aproximar todos los criterios interpretativos surgidos de la realización práctica del tratamiento de datos de ADN, en su memoria del año 2003. Explica esta Institución que "los datos biométricos proporcionan una identificación inequívoca de las personas en base a rasgos que les son consustanciales" y, distingue entre la verificación de la identidad de una persona concreta y, distingue la información de todo su grupo genético, su salud (presente y futura) y la de sus familiares, de tal forma que tiene en cuenta que los datos genéticos pueden ser obtenidos con facilidad, que pueden revelar mucha información de la persona y, que puede ser utilizados por un número creciente de organismos, para fines muy diversos. Por ello, señala que "la adecuada protección de los datos genéticos, puede considerarse hoy día un requisito previo en orden a garantizar el respeto al principio de igualdad y, convertir en una realidad el derecho a la salud".

Según la AEPD, "las autoridades de protección de datos consideran que cualquier uso de los datos genéticos para fines distintos de la salvaguardia de la salud del sujeto de los datos o la investigación científica, debe estar sometido a normas nacionales que lo regulen, de acuerdo con los principios de protección de los datos y, en particular, con los principios de finalidad y proporcionalidad lo que implicaría la ilicitud de la puesta en práctica global de pruebas genéticas en masa." De ahí que deba considerarse su tratamiento como una excepción a la regla general de su prohibición, evitando especialmente todo tipo de discriminaciones de base biológica entre los distintos tipos de perfiles genéticos que configuran el grupo humano, e incluso usurpaciones de identidad o clonaciones"[692]. *Como* "tal particularidad, debe por tanto ser delimitada por las normas legales de cada país y, "configurado el status jurídico de las muestras de ADN, con la mayor precisión. Es preciso encontrar el equilibrio entre el derecho del

[692] Por ejemplo: la Agencia Española de Protección de Datos desestimó la creación de un fichero con muestras genéticas para identificar a recién nacidos por medio de pruebas de ADN. El objetivo de tales ficheros hubiera sido impedir los errores de identificación madre-hijo. La Agencia Española de Protección de Datos opinó que la creación de un fichero genético sería contraria al principio de proporcionalidad en la medida en que pueden obtenerse resultados idénticos de manera fiable por otros medios como, por ejemplo, mediante pulseras de identidad o huellas plantares. El criterio de proporcionalidad ha sido primordial en la mayoría de las decisiones tomadas hasta ahora por las autoridades de protección de datos sobre el tratamiento de los datos genéticos.

individuo a decidir sobre su propia información personal y, los derechos de quienes se podrían ver afectados por su tratamiento como consecuencia de alcance colateral".

En consecuencia, la familia biológica es la que presenta mayores dificultades en orden a la delimitación del derecho a decidir, pero las autoridades de protección de datos lo dejan en el aire y consideran que, "debería de realizarse un enfoque caso por caso a la hora de decidir cómo tratar los posibles conflictos entre los intereses de los sujetos de los datos y los de su familia biológica".

En el aspecto que nos ocupa, de tratamiento de la información genética para fines policiales, la AEPD, es consciente de que "desde los atentados terroristas del 11 de septiembre de 2001 en los Estados Unidos de América, se han ido adoptando progresivamente toda una serie de medidas encaminadas a incrementar la cooperación internacional en la lucha contra el terrorismo y las formas graves de delincuencia organizada transnacional" y esto, en la UE, se ha traducido en conjunto de Convenios suscritos para reforzar el espacio de libertad, seguridad y justicia, siempre aplicables dentro del estricto marco de respeto de los derechos y libertades fundamentales de los europeos. Para ello, las autoridades de protección de datos de los Estados miembros juegan un papel esencial, a la hora de mejorar la cooperación de todos los servicios policiales en la lucha contra el terrorismo y el crimen organizado y, recordando que las posibilidades de intercambio de información están restringidas para unos fines concretos, a una serie de organismos concretos y, por el absoluto respeto a los derechos en materia de protección de datos de las personas.[693]

[693] "Dentro de los desarrollos operativos, hay que mencionar la continuación de los trabajos para el desarrollo de lo que se ha dado en llamar SIS II, es decir, el Sistema de Información Schengen de segunda generación que, desde el punto de vista jurídico, han venido acompañados por una iniciativa española de modificación del Convenio de Aplicación del Acuerdo de Schengen que ya fue comentada en la anterior Memoria. La ACC Schengen ha seguido de cerca los trabajos encaminados a modificar el actual Sistema de Información Schengen (SIS) por uno nuevo denominado SIS II, cuya entrada en funcionamiento está prevista para el año 2006. Las razones esenciales para sustituir el sistema son la ampliación de la Unión Europea que acarrea la necesidad de procesar mayor cantidad de información y la adición de nuevas funcionalidades para mejorar la lucha contra el crimen y el terrorismo. La ACC ha venido planteando que la modificación de la naturaleza del SIS como herramienta de investigación policial, requiere la realización de un estudio que analice el impacto que producirá sobre los derechos de las personas. […]. Por lo que respecta al ámbito de Europol, en el año 2002 se produjo una iniciativa del Reino de Dinamarca con vistas a modificar el Convenio Europol para, teniendo en cuenta la experiencia adquirida durante los primeros años de existencia de dicha institución y las nuevas necesidades de la

3.3 - Europa: Grupo de Trabajo del Artículo 29 y Tratado de Prum.

Desde Europa viene además marcada una línea directriz de la situación normativa del tratamiento de datos genéticos, para todos los Estados Miembros. En el año 2004, el Grupo de Trabajo del Artículo 29 sobre protección de datos, publicaba un Documento con recomendaciones sobre el tratamiento de datos genéticos (adoptado el 17 de marzo de 2004)[694], en el que mostraba su preocupación por los progresos tecnológicos y de la ciencia, en el ámbito de la investigación genética, por "nuevas cuestiones y preocupaciones en materia de protección de datos, por lo que se refiere a la importancia y el impacto de las pruebas genéticas y el tratamiento de los datos genéticos". Se destacaba en este estudio general que la situación en la UE no es homogénea, porque si bien es cierto, que algunos Estados miembros otorgan explícitamente a los datos genéticos un carácter sensible, la mayoría de los Estados miembros ni siquiera lo tiene regulado por una legislación específica.

Sin embargo, es patente que los Estados son cada vez más conscientes de los riesgos vinculados al tratamiento de los datos genéticos y, en general, en el campo de la salud, y así las recomendaciones y estudios del Grupo de Trabajo del Artículo 29, se han dirigido a sopesar los riesgos y derechos en conflicto en los tratamientos de este tipo de datos, que considera sin duda de marcado carácter sensible[695]. Bajo esta premisa,

---

lucha contra el crimen organizado y el terrorismo internacionales, adaptar el mismo para dar una mejor respuesta a dichas necesidades. La ACC Europol emitió su primer dictamen sobre esta propuesta en octubre de dicho año. Este dictamen junto con las negociaciones que se fueron desarrollando, dio origen a un nuevo texto sobre el que el Consejo alcanzó un acuerdo general en diciembre del año 2002. Sobre este nuevo texto se pronunció de nuevo la ACC Europol en marzo del año 2003 manifestando que hay que hacer hincapié en que para luchar eficientemente contra las formas graves de delincuencia internacional organizada se requiere un esfuerzo conjunto entre Europol y los Estados miembros para mantener unos estándares de tratamiento de la información adecuados y, en particular, para garantizar la confidencialidad, fiabilidad y calidad de la información de acuerdo con las normas de protección de datos aplicables. La intención de interconectar los sistemas de Schengen, Europol y Eurojust subraya la necesidad de este esfuerzo conjunto". MEMORIA año 2003, Ed. Agencia Española de Protección de datos (2003), pp. 73 y 74.

694 Grupo de Trabajo del Artículo 29 sobre protección de datos. Documento de trabajo sobre datos genéticos. Op. Cit.

695 En especial, el Convenio sobre los Derechos Humanos y la Biomedicina, adoptado en Oviedo en 1997, instrumento de carácter vinculante internacional y, abierto desde entonces a su adhesión y a su

considera que deben ser de obligada observancia todas las conclusiones - recomendaciones que recoge su Documento de Trabajo del año 2004, pues, concretamente en tratamientos de datos genéticos para fines policiales, son del todo aplicables a la situación actual en Europa y las medidas de investigación que se vienen adoptando en las investigaciones sobre terrorismo y bandas de delincuencia organizada, situaciones extremas por la inevitable necesidad de compensar riesgos para la seguridad y, por la excepción que conlleva para el libre ejercicio de derechos fundamentales. Por tanto, para poder hablar de un equilibrio medio de intereses, se debe hacer referencia expresa a las recomendaciones de este Grupo de Trabajo, que son:

> "a) evaluar el respeto de la proporcionalidad y la legitimidad, habida cuenta de los riesgos en materia de protección de los derechos fundamentales y de la libertad de las personas y, en particular, si el objetivo inicial no hubiera podido alcanzarse de una manera menos intrusista;
>
> b) la aplicación de disposiciones nacionales que regulen los usos de los datos genéticos distintos de la protección de la salud del interesado y la investigación científica, de conformidad con los principios de la Directiva sobre protección de datos y, en particular, los principios de finalidad y proporcionalidad. La aplicación de tales principios confiere carácter ilegal a la aplicación global de pruebas genéticas de masa;
>
> c) deben definirse procedimientos que garanticen que los datos genéticos sólo se tratarán bajo el control de expertos cualificados, habilitados a efectuar estos tratamientos en virtud de autorizaciones y normas específicas;
>
> d) que los Estados miembros examinen la posibilidad de que el tratamiento de datos genéticos dependa del control previo de las

ratificación. Prohíbe toda forma de discriminación contra una persona debido a su patrimonio genético y sólo autoriza las pruebas predictivas con fines médicos.

autoridades de protección de los datos […] esto debería aplicarse a la creación y utilización de "biobancos".

Siguiendo esta línea se pronunció por ejemplo, el TEDH en el asunto S. y Marper contra Reino Unido, en relación con la conservación de perfiles de ADN o de huellas dactilares de una persona absuelta de un delito o, en relación a la cual, el procedimiento se hubiese archivado antes de dictarse condena. El Tribunal consideró que dicha restricción del derecho a la intimidad sólo puede justificarse si responde a una necesidad social acuciante, si es proporcional al objetivo perseguido y, si las razones expuestas por la autoridad pública para justificarla son pertinentes y suficientes. Los principios básicos de la protección de datos exigen que la conservación de datos sea proporcionada en relación con la finalidad de su recogida, y que el período de almacenamiento sea limitado[696]

El principal acuerdo que recoge las concretas bases de cooperación entre los Estados miembros de la UE, es el conocido "Tratado de PRUM", que se planteó para determinar el procedimiento de cooperación que deben seguir sus autoridades policiales, para el tratamiento e intercambio de información de carácter genético de sus ciudadanos, teniendo en cuenta siempre que los citados principios de límite y respeto a los derechos de los individuos sobre su propia información personal, son de ineludible cumplimiento.

Este Tratado, conocido como "Schengen III", fue elaborado entre la República Federal Alemana, Bélgica, España, Luxemburgo, los Países Bajos y Austria, y en mayo de 2005 fue ratificado por España. Su articulado nació para sentar una regulación que reforzase la cooperación transfronteriza para luchar con mayor firmeza contra el terrorismo, el crimen organizado y la inmigración irregular, y para ello promovió la creación de bases de datos de ADN en cada país.

[696] Asunto Marper contra Reino Unido, Sentencia de 4 de diciembre de 2008. TEDH. pp. 30 y 31.

El artículo 2 de este texto internacional, se estableció expresamente para dotar de un marco legal preciso a la creación de ficheros nacionales de análisis del ADN, y así, su redacción señala el compromiso de las "partes contratantes para crear y mantener ficheros nacionales de análisis del ADN para los fines de la persecución de los delitos". Pero matiza que el "tratamiento de los datos almacenados en esos ficheros (…) se llevará a cabo con arreglo al derecho interno vigente para cada tipo de tratamiento", es decir, se configura desde el principio como una regulación de mínimos que obviamente necesitará ser detallada en cada Estado involucrado de forma activa en el acuerdo. En cualquier caso, respecto de la elaboración de un entorno restringido para el tratamiento y consulta de bases de datos genéticos, el Tratado señala una serie de límites prácticos que no podrán ser rebasados por los Estados firmantes, como por ejemplo, que los sistemas implantados (basados en índices de referencia, tratamientos disociados) para el tratamiento de datos genéticos, exclusivamente se compongan de perfiles de ADN obtenidos a partir de la parte no codificante del ADN, es decir, que no podrán contener datos que permitan identificar directamente a la persona concernida y, en el caso de datos que no pudieran atribuirse a ninguna persona ("huellas abiertas"), deberán poder reconocerse como tales.

El artículo 3 contempla la posibilidad del intercambio de la información de manera automatizada en el "derecho a consultar los datos", mediante una comparación de perfiles de ADN y/o datos dactiloscópicos[697]. En este caso, el límite está en que la consulta deberá formularse únicamente para casos concretos y, con arreglo al derecho del Estado que realice la consulta para su comparación. Cuando se haya obtenido la información interesada, el Estado requirente realizará la comparación también de forma automatizada (artículo 4) y, si constata la coincidencia del algún perfil de ADN con los existentes en sus propios ficheros de análisis del ADN, entonces deberá comunicarlo sin demora al Estado "requerido" para que éste pueda (artículo 5) proceder a la correspondiente la transmisión del resto de los

[697] Cuyo origen puede señalarse en el sistema EURODAC. Eurodac es una base de datos europea de impresiones dactilares creada exclusivamente con el fin de identificar a las personas solicitantes de asilo. Este sistema de identificación automática de impresiones dactilares, comenzó a funcionar el 15 de enero de 2003, y fue el primero de este tipo creado en la Unión Europea. En la actualidad, todos los Estados miembros, excepto Dinamarca, participan en esta iniciativa.

datos de carácter personal disponibles, relativos a los índices de referencia y demás informaciones identificadoras del sujeto en cuestión. Para tramitar todo este proceso de intercambio de datos, cada estado debe designar un "punto de contacto" (artículo 6) y un "acuerdo de ejecución" propio, con arreglo a su derecho interno.

Respecto de la formación de las bases de datos nacionales, el artículo 7 señala que para la "obtención de material genético molecular y transmisión de perfiles de ADN (…), si en el curso de una investigación o procedimiento penal no se dispone del perfil de ADN de una persona determinada, que se encuentre en el territorio de un Estado parte del Tratado, éste deberá prestar asistencia judicial mediante la obtención y el análisis de material genético molecular de dicha persona y, la transmisión del perfil de ADN resultante". Esta colaboración será obligatoria siempre que se realice en atención a "una orden o declaración de investigación de la autoridad competente del Estado que la requiera, y se realizará de conformidad con la normativa interna del estado requerido".

En general, se establece un esquema orientativo para sistematizar la consulta e intercambio de información genética (perfiles genéticos e inventarios de huellas) entre los Estados firmantes. El acuerdo ratificado pretende, en definitiva, agilizar el intercambio de información sobre individuos relacionados con actividades terroristas y, el intercambio de información que prevenir o atender catástrofes.

3.4.- La Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

El día 9 de octubre de 2007, se publicó en el Boletín Oficial de Estado[698], la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. Este texto normativo, pretende marcar un hito en España respecto de la toma de conciencia sobre la trascendencia de los marcadores genéticos en las investigaciones criminales y, sobre la necesidad de utilizarlos siempre en un ambiente de respeto a los derechos fundamentales de los individuos afectados. Según su propia Exposición de Motivos, ello viene dado "tanto por el carácter sensible que dichos datos tienen y el importante grado de protección con que, naturalmente, deben contar, como por la inexistencia de un marco jurídico que regule adecuadamente su empleo". La Disposición Final Primera de la Ley Orgánica 15/2003, de 25 de noviembre, de modificación del Código Penal, reformó la Ley de Enjuiciamiento Criminal (arts. 326 y 363) para dar cobertura a la "posibilidad de obtener el ADN a partir de muestras biológicas provenientes de pruebas halladas en el lugar del delito o extraídas de sospechosos, de manera que dichos perfiles de ADN puedan ser incorporados a una base de datos para su empleo en esa concreta investigación". El problema es que esta reforma no contempló las posibilidades de tratamiento automatizado de este tipo de datos personales, y esto, unido a la ratificación del Tratado de Prum por España, en Mayo de 2005, exigía ya una regulación precisa de dichos tratamientos, sobre todo, un marco legal que permita realmente "crear una base de datos en la que, de manera centralizada e integral, se almacenase el conjunto de los perfiles de ADN obtenidos, a fin de que pudiesen ser utilizados, posteriormente, en investigaciones distintas o futuras, incluso sin el consentimiento expreso del titular de los datos".

[698] B.O.E nº 242, de 9 de Octubre de 2007, p. 40969.

En la inicial declaración de intenciones de esta Ley, el legislador asume que este marco normativo que va a establecer es necesario por los inevitables avances técnicos, la exigencia social de facilitar los instrumentos de investigación más eficientes posibles y, "la creciente globalización de los delitos y la paralela asunción por parte de España de una serie de obligaciones recíprocas con otros países[699]". Destaca en este cometido, como objetivo principal de la nueva norma: "la creación de una base de datos en la que, de manera única, se integren los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado en los que se almacenan los datos identificativos obtenidos a partir de los análisis de ADN que se hayan realizado en el marco de una investigación criminal, o en los procedimientos de identificación de cadáveres o de averiguación de personas desparecidas".

Si bien es cierto que era importante contar con este instrumento legal, se echa de menos la elaboración de una Ley Orgánica específica, que refundiese los textos legales existentes en España sobre tratamiento de material genético, incluyendo cada especialidad (entorno laboral, médico, policial, etc.) y sus excepciones tasadas, así como las posibilidades de interacción entre bases de datos genéticos creadas con distinta finalidad y, las bases de datos centralizadas creadas con fines de cooperación internacional. Es sabido que toda forma de "parcheo" legal implica la inevitable apertura de nuevas lagunas legales y de posibles intromisiones en ámbitos protegidos por los derechos de los individuos, en consecuencia, quedan aún en el aire riesgos innecesarios, máxime cuando la licencia para ello viene de la mano de un interés general de la talla de la "lucha contra el terrorismo".

En cualquier caso, se viene a delimitar el tratamiento de datos genéticos, especialmente para "aquellos perfiles de ADN que sean reveladores, exclusivamente, de la identidad del sujeto -la misma que ofrece

[699] "Cabe señalar que la adopción de esas medidas jurídicas, así como la creación de bases de datos que permitan intercambiar la información entre los Estados miembros, ha sido reiteradamente expuesta desde las Instituciones comunitarias a través de sendas Resoluciones del Consejo relativas al intercambio de resultados de análisis de ADN, de 9 de junio de 1997 y de 25 de julio de 2001, respectivamente. En el mismo sentido se ha venido pronunciando el Consejo de Europa a partir de la Recomendación (92) 1, de 10 de febrero de 1992, de su Comité de Ministros, sobre la utilización de los resultados de análisis de ADN en el marco del sistema de justicia penal". Exposición de Motivos del Proyecto de Ley Reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. B.O.E. num. 117-1, de 15 de diciembre de 2006 (apartado primero).

una huella dactilar- y del sexo, pero, en ningún caso, los de naturaleza codificante que permitan revelar cualquier otro dato o característica genética y, tanto para la investigación y averiguación de delitos, como para los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas", y ello siempre dentro del marco legal establecido por la LOPD, "la cual, por su propia naturaleza de regulación general en la materia, resulta de aplicación directa, siendo los preceptos de esta Ley especialidades permitidas por la citada Ley Orgánica, que encontrarían su justificación en las peculiaridades de la base de datos que regula".

El articulado de la Ley, está elaborado con un orden sistemático y ascendente en nivel de concreción, que comienza relatando los requisitos de la creación de la base de datos centralizada, continúa señalando los órganos competentes para su tratamiento, y termina especificando una serie de reglas de obligada observancia para dicho tratamiento.

El artículo 1 establece que por esta nueva norma se crea "la base de datos policial de identificadores obtenidos a partir del ADN, que integrará los ficheros de esta naturaleza de titularidad de las Fuerzas y Cuerpos de Seguridad del Estado tanto para la investigación y averiguación de delitos, como para los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas". Y añade el artículo siguiente que su gestión dependerá del Ministerio del Interior.

En los siguientes preceptos, se citan los distintos tipos de identificadores obtenidos a partir del ADN, la finalidad exclusiva de su inclusión en la base de datos policial y los laboratorios acreditados para configurar en general la información que contendrán.

La finalidad se establece con claridad y precisión, pues va a marcar los límites del tratamiento y la calidad de los datos a tratar desde el origen. Se determina que sólo podrán inscribirse en los identificadores obtenidos, "en el marco de una investigación criminal, que proporcionen, exclusivamente, información genética reveladora de la identidad de la persona y de su sexo". Este supone uno de los requisitos fundamentales

para poder proceder al tratamiento de datos genéticos si tenemos en cuenta que, la inscripción en la base de datos policial de los identificadores obtenidos a partir del ADN, "no precisará el consentimiento del afectado", sin embargo, esto no exime de la obligación de informar por escrito al afectado "de todos los derechos que le asisten respecto a la inclusión en dicha base". De la estricta observancia de estos preceptos va a depender en gran medida la garantía de los derechos fundamentales de la persona, de ahí que debiera haberse previsto, tanto la finalidad como la exclusión del consentimiento, en una norma de rango superior, en una Ley Orgánica, que en conclusión contemplase taxativamente las excepciones y límites al ejercicio de los derechos de los afectados.

Respecto del tratamiento en si, los artículos 6 a 8 exigen el establecimiento de garantías específicas para el traslado, conservación y custodia de la información genética, exigen también el establecimiento de medidas de seguridad de nivel alto[700] para todos los ficheros que integren la base de datos, y, exigen que para el uso y cesión de los datos se respete la competencia de la autoridad policial u organismos autorizados[701].

Finalmente, se dedica tan sólo un precepto a recordar los derechos de los afectados por este tipo de tratamientos (el artículo 9): los derechos de acceso, rectificación y cancelación, limitados en todo caso por la duración del correspondiente procedimiento en que estén siendo utilizados o, la prescripción del delito investigado y, matiza que en "todo caso se procederá a su cancelación cuando se hubiese dictado auto de sobreseimiento libre o sentencia absolutoria (…) una vez que sean firmes dichas resoluciones. En el caso de sospechosos no imputados, la cancelación de los identificadores inscritos se producirá una vez que hubiese recaído resolución firme que impida el enjuiciamiento de los mismos".

[700] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[701] Hay que destacar el límite expreso que impone el apartado segundo del artículo 7, a la interacción de informaciones para la investigación policial al señalar que, una vez más, la finalidad del tratamiento determinará las posibilidades de uso y cesión: "cuando el tratamiento se realizase para la identificación de cadáveres o la averiguación de personas desaparecidas, los datos incluidos en la base de datos objeto de esta Ley sólo podrán ser utilizados en la investigación para la que fueron obtenidos".

Este precepto hace además mención especial a los datos de las personas fallecidas, datos que son ajenos a la Ley de Protección de Datos y que, en materia de información genética, de mantenerse, podrían tener una gran trascendencia sobre los herederos naturales del material genético del afectado. Por este motivo, se señala que los "datos pertenecientes a personas fallecidas se cancelarán una vez el encargado de la base de datos tenga conocimiento del fallecimiento". Sin embargo, en los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o, de averiguación de personas desaparecidas, "los datos inscritos no se cancelarán mientras sean necesarios para la finalización de los correspondientes procedimientos".

Por último, se mencionan los supuestos específicos de los "identificadores obtenidos a partir del ADN respecto de los que se desconozca la identidad de la persona a la que corresponden, que permanecerán inscritos en tanto se mantenga dicho anonimato. Una vez identificados, se aplicará lo dispuesto en este artículo a efectos de su cancelación".

Todo lo expuesto sobre el tratamiento de datos genéticos con finalidades policiales, es exclusivamente aplicable en coherencia la normativa de protección de datos, tanto la Ley 15/1999 de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, como la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Lo cierto es que a pesar de lo expuesto se mantiene cierto vacío legal y de garantías, debido a la amplitud de tratamientos que ofrece la información genética. Y es que, aun tratándose tan sólo de aquella parte del código genético que identifica al sujeto, no puede olvidarse que se trata de una información muy valiosa que, mal utilizada, puede provocar graves perjuicios para el afectado derivando incluso en situaciones discriminatorias de difícil reparación. Como se ha comentado, en el caso de las investigaciones de terrorismo o de delincuencia organizada, la amplia carta

de excepciones existente puede llegar a suponer la desprotección de quienes se vean involucrados (recuérdese que lo sean como simples "sospechosos"), incluso a nivel internacional. Tal vez los pasos que el legislador español va dando quieran completar lo ya existente, pero lo cierto es que un texto refundido, adecuado por la materia fundamental que trata, despejaría tanto los límites como las garantías ya previstos por nuestro ordenamiento y, por el ordenamiento comunitario e internacional, aunque también es cierto que dejaría al descubierto las carencias normativas y de conciencia aún latentes.

4. "Passenger Name Record" (PNR).

Los conceptos de intimidad en la Unión Europea y, de seguridad nacional en los Estados Unidos, vieron enfrentados sus pilares normativos tras los atentados del 11 de septiembre de 2001 en Nueva York. La puesta en marcha de diferentes mecanismos de control y vigilancia sobre la información de los ciudadanos en el territorio estadounidense, afectaba de forma directa a ciudadanos de la Unión Europea.

En Estados Unidos el régimen jurídico de la protección de la intimidad no tiene el mismo compromiso que la Unión Europea, y la crisis de seguridad del 11-S, supuso que empezaran a disponer de todo tipo de tecnologías que permitieran detectar la actividad terrorista y proteger la seguridad pública, en especial, la seguridad de las fronteras y la seguridad del transporte aéreo.

Uno de los primeros proyectos en ese sentido fue el "Total Information Awareness" (Conocimiento Total de la Información) del Departamento de Defensa, que luego pasaría a llamarse "Terrorism Information Awareness" (Conocimiento de Información sobre el Terrorismo), y cuya finalidad era controlar posible actividad terrorista en la aviación nacional e internacional, controlando la información de bases de datos

personales, tanto comerciales como del Gobierno. Respecto de la aviación nacional, en el año 2001 se implantó el Sistema Informatizado de Preselección de Pasajeros (CAPPS II)[702], que daba acceso a las bases de datos de las reservas de vuelo que hicieran los pasajeros y mediante el cual, tras comprobar la identidad del pasajero, se analizaría el riesgo que supondría dejarle subir a un avión. Respecto a la aviación internacional, el Congreso de los Estados Unidos aprobó la Ley de Seguridad de la Aviación y del Transporte[703], en noviembre de 2001. Esta norma nació envuelta en todo tipo de críticas, por cuanto exigía que las líneas aéreas con destino a EEUU tuvieran a disposición del Servicio de Aduanas y Protección de Fronteras (Bureau of Customs and Border Protection – CBP) toda la información de la lista de pasajeros, para ser trasmitida por medios electrónicos a petición del CBP, antes de que el avión llegase a EEUU. En concreto, este tipo de actuaciones, así previstas, se consideraban del todo incompatibles con el sistema europeo de protección de dato de la UE, dónde es ilegal realizar transferencias de datos de carácter personal a países que no reúnan las condiciones necesarias de una "adecuada" protección de la intimidad, en materia de datos personales[704].

Posteriormente, otro programa de protección y seguridad nacional que afectaba al transporte de pasajeros, fue el Programa de Tecnología de Indicador de Situación de Visitantes e Inmigrantes de los Estados Unidos, conocido como US VISIT ("United States Visitor and Immigrant Status Indicator Technology")[705], cuya primera fase entró en vigor en enero de

---

[702] El primer sistema de preselección de pasajeros se implantó en 1998, en el seno de la actividad de la Comisión de Seguridad de la Aviación (1996-1997), tras el accidente de aviación del vuelo 800 de la TWA en 1996, en Long Island (Nueva York). Esta Comisión estaba presidida por Al Gore, y su principal misión era asignar códigos a los datos de reserva de los pasajeros de un vuelo al realizar la facturación, que era cotejada con una lista de "exclusión aérea", de personas vigiladas por el FBI. Véase Edward HASBROUCK, "*Total Travel Information Awareness*", disponible en la página web del Gobierno de EEUU, *Transportation Security Administration* (TSA) http://www.Hasbrouck.org/articles/travelprivacy.html

[703] *Aviation and Transportation Security Act*. Disponible en: http://www.tsa.gov/research/laws/law_regulation_rule_0010.shtm

[704] El 14 de mayo de 2002, los Estados Unidos aprobaron otra ley para reforzar la seguridad fronteriza, que exige que las compañías aéreas que entren y salgan de este país transmitan los datos relativos a los pasajeros y la tripulación al US Immigration and Naturalization Service5 (Servicio de Inmigración y Naturalización de los EE.UU.). En lo que respecta a los pasajeros y la tripulación que salgan de los EE.UU. *Enhanced Border Security and Visa Entry Reform Act of 2002*. Pub. L. No. 107-173 (H.R. 3525) Section-by-Section Explanation. Disponible en: http://www.ofr.harvard.edu/additional_resources/Summary_of_Enhanced_Border_Security_Reform_Act_HR3525.pdf

[705] Diseñado para desarrollar procesos de entrada y salida e integrar datos y procesos de inmigración con otras agencias del DHS, entre las cuales se encuentran: la CBP, la Oficina de Inmigración y Aduanas (Immigration and Customs Enforcement - ICE), USCIS y la Administración de Seguridad para el

2004. Su particularidad residía en que al solicitar un visado para entrar en EEUU, se realiza una recogida de datos tanto del viaje como del viajero, datos biométricos. Se realiza un escaneo del dedo índice de las dos manos y una fotografía digital del rostro del solicitante, para incluirlos en una base de datos del Departamento de Estado ("Department of Homeland Security"), y poder así realizar comparaciones con la base de datos de personas peligrosas del Gobierno.

El Gobierno de los Estados Unidos tenía interés en dos categorías de datos. La primera, la conocida como PNR ("Passenger Name Record"), información de registro del pasajero en la base de datos de reservas de la compañía aérea. Los datos que incluye, son el nombre del pasajero, su dirección postal, su dirección de correo electrónico y su número de tarjeta de crédito. Otros datos, relativos al viaje, como reservas de hotel y de alquiler de coche, las preferencias alimenticias e información sobre las discapacidades que tenga el pasajero, e incluso relativos a viajes anteriores, como vuelos realizados, vuelos cancelados o no realizados a pesar de la reserva, los números de las tarjetas de crédito utilizadas, etc.

La segunda, conocida como API ("Advance Passenger Information"), información anticipada de pasajeros, es más limitada, incluye datos como nombre de la persona, fecha de nacimiento, nacionalidad, género, país emisor del pasaporte o visado y número de los documentos, número de vuelo del pasajero, aeropuerto de salida y aeropuerto de llegada.

Este tipo de tratamientos, la recogida y almacenamiento de estos datos por Estados Unidos, encontraron el principal obstáculo a la internacionalización, en sus relaciones con la Unión Europea. Las tensiones, comenzaron con un primer acuerdo, provisional, celebrado entre la Comisión Europea y el Servicio de Aduanas de los Estados Unidos (que forma parte del Departamento de Seguridad nacional): la "Declaración Conjunta sobre información de Registro del Nombre del Pasajero", de 17 de Marzo de 2003.

Transporte (Transportation Security Agency - TSA). US-VISIT trabaja también asociado con el Departamento de Estado (Department of State - DOS), el Departamento de Justicia (Department of Justice -DOJ), y el Departamento de Transporte (Department of Transportation - DOT). Detalles del programa, disponibles en:
http://www.dhs.gov/files/programs/usv.shtm

En sus considerandos preveía que los datos recogidos sólo podrían usarse para "objetivos de mantenimiento del orden", para combatir el terrorismo y otras ofensas criminales graves, que se implantarían un sistema de extracción de datos de las compañías aéreas ("pull system"), y que podrían retenerse todo el tiempo "requerido para el propósito con el que se almacenaron", cuestiones por las que comenzaron las críticas[706].

El entonces Presidente del Grupo de Trabajo del Artículo 29, Stefano RODOTÁ, expuso al Presidente de la de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE), su disconformidad con este acuerdo, y la necesidad de clarificar la base legal de las transferencias de datos, por cuanto se estaba obligando a otros países a respetar las leyes de EEUU[707]. Puso de relieve que si bien "los Estados soberanos poseen un criterio definido respecto a la información que pueden pedir a las personas que desean acceder a su territorio, sin embargo, las propuestas actuales en lo que respecta al sistema APIS, si bien se han elaborado en el contexto de abominaciones terroristas, podrían llevar a la divulgación desproporcionada y periódica de información por parte de las compañías aéreas que deben atenerse a los requisitos de la Directiva 95/46/CE. Esta información podría utilizarse con fines regulares relacionados con la inmigración y el control aduanero así como, de un modo más general, para la seguridad nacional de los EE.UU., y podría al menos ser compartida por todas las agencias federales de dicho país".

Y respecto a la fórmula del acuerdo "unilateral", entendía que debía "adoptarse una perspectiva global para tratar la transferencia de datos personales por parte de las compañías aéreas a los Estados Unidos. En primer lugar, sería necesario tener en cuenta otras transferencias, existentes o planeadas, a dicho país. Sería especialmente necesario

[706] European Commission/US Customs Talks on PNR Transmission, Brussels, 17/18 February Joint Statement. Disponible en: http://www.statewatch.org/news/2003/feb/11usdata2.htm

[707] "El Grupo se pregunta hasta qué punto estas medidas, aprobadas unilateralmente, son compatibles con los acuerdos y convenios internacionales sobre tráfico y transporte aéreo, así como con el Derecho nacional aplicable respecto a aquellos países en los que las compañías aéreas operan permanentemente. (…) Los datos facilitados por las compañías aéreas se refieren a personas físicas identificadas. Estos datos son tratados por compañías en la UE (recogidos, registrados, modificados, almacenados, nuevamente modificados, solicitados, utilizados, reenviados, etc.). Como tales, están protegidos por las disposiciones de la Directiva 95/46/CE. Véase la Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos". Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp66_es.pdf

incorporar el concepto de tercer pilar. Esencialmente, las transferencias de datos a las autoridades públicas de terceros países por razones de orden público en este país deberían ser entendidas en el contexto de los mecanismos de cooperación establecidos por medio del tercer pilar (cooperación judicial y policial). Asimismo, estos mecanismos deberían estar estrechamente relacionados con las garantías de la protección de los datos transferidos. Parece resultar importante para el buen funcionamiento de los mecanismos de cooperación basados en el tercer pilar que no se esquiven pasando, en su lugar, por el primer pilar. Por último, la solución a la que se llegó para las transferencias de datos a los Estados Unidos podría resultar apropiada para servir de modelo a las transferencias que se realizan a terceros países distintos a través de APIS".

El Parlamento Europeo, tampoco se mostró conforme con las directrices de dicho acuerdo, y en una Resolución del año 2003[708] expuso su malestar por el retraso con que la Comisión había planteado el problema, considerando que afectaba a "otras políticas de la Comunidad (transportes, inmigración) y de la Unión (cooperación policial y judicial o lucha contra el terrorismo y la delincuencia organizada)", y la falta de diligencia demostrada en la supervisión del Derecho Comunitario

> - "no verificando si el acceso a los datos de los sistemas de reserva tiene una base real en la legislación de los Estados Unidos o se trata de una interpretación extensiva por parte del Gobierno de este país(11); pide, por otra parte, a la Comisión que aproveche los debates actualmente existentes en los Estados Unidos sobre la nueva legislación respecto al APIS y al PNR, de modo que logre de las autoridades de los Estados Unidos que esta nueva legislación tenga en cuenta las exigencias de protección de datos que se derivan de la legislación comunitaria;

[708] Resolución del Parlamento Europeo sobre la transmisión de datos personales por las compañías aéreas en los vuelos transatlánticos. P5_TA(2003)0097; B5-0187/2003. Disponible en: http://www.europarl.europa.eu/pv2/pv2?PRG=DOCPV&APP=PV2&SDOCTA=5&TXTLST=1&TPV=PROV&POS=1&Type_Doc=RESOL&DATE=130303&DATEF=030313&TYPEF=B5&PrgPrev=TYPEF@B5|PRG@QUERY|APP@PV2|FILE@BIBLIO03|NUMERO@187|YEAR@03|PLAGE@1&LANGUE=ES

- retrasando la verificación prevista por el artículo 25 de la Directiva 95/46/CE de la legislación de los EE.UU.; un retraso crea dificultades evidentes a las compañías aéreas que se ven atrapadas en la disyuntiva de incurrir en las sanciones estadounidenses (si respetan el Derecho comunitario) y la penalización de las autoridades en materia de protección de datos (si acceden a las exigencias de las autoridades estadounidenses), y crea también dificultades a las autoridades nacionales en materia de protección de datos, que deben velar por el respeto de las disposiciones comunitarias;

- no informando a los ciudadanos, que deberían ser los primeros en conocer el destino de las informaciones que les afectan*".*

El Parlamento además señaló que a su entender, la declaración conjunta de los funcionarios de la UE y de los EE.UU., de 19 de febrero de 2003, carecía de fundamento jurídico y podía llevar a interpretaciones libres, como aparentar una invitación indirecta a las autoridades nacionales a no respetar el Derecho comunitario. Consideraba que las negociaciones, debían respetar "las competencias comunitarias en materia de transportes aéreos (...) para las que la Comisión está dispuesta a negociar un acuerdo de 'cielos abiertos' ('open skies')", así como las competencias en materia de política de inmigración, y pidió expresamente a la Comisión que suspendiera "los efectos de las medidas adoptadas por las autoridades estadounidenses hasta que se adopte la decisión sobre la compatibilidad de dichas medidas con el Derecho comunitario".

Estas duras críticas, fueron también respaldadas por el Grupo de Trabajo del Artículo 29. En su Dictamen 4/2003 relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de pasajeros, de 13 de junio de 2003[709], exponía su preocupación, porque consideraba un objetivo prioritario "establecer, lo antes posible, un marco jurídico claro para todas las transferencias de datos de las compañías aéreas

[709] Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach.
Disponible en: http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0826en01.pdf

a los EE.UU. que sea compatible con los principios relativos a la protección de los datos. Aunque reconoce que en última instancia habrá que atender a consideraciones de carácter político, el Grupo insta a la Comisión a tener sus opiniones plenamente en cuenta en las negociaciones con las autoridades estadounidenses. El Grupo es consciente de que podría ser necesario aplicar un enfoque más general en relación con las condiciones de uso de los datos del transporte aéreo con fines de seguridad en un contexto multilateral".

Se consideraba estrictamente necesario además, limitar los fines para los que se podían utilizar los datos recabados, limitar el número y categoría de los datos, disponer de un formulario de información a los pasajeros de sus derechos (acceso, rectificación y reparación), e implantar un sistema "push" que permitiera a las compañías aéreas enviar los datos, en vez de dar acceso a las autoridades estadounidenses.

Finalmente, el 16 de diciembre de 2003, la Comisión Europea emitió un informe[710] para el Parlamento y el Consejo, informando de que a pesar de haber llegado a un acuerdo con Estados Unidos, seguiría trabajando en la consecución de un sistema de transferencia de datos de pasajeros que respetase la normativa europea.

La reacción del Grupo de Trabajo del Artículo 29 no se hizo esperar, y con fecha 29 de enero de 2004, emitió su opinión en el Dictamen 2/2004 sobre el carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros (Passenger Name Records, PNR) que se transfieren al Servicio de aduanas y protección de fronteras de Estados Unidos (Bureau of Customs and Border Protection, CBP)[711]. En él, reconocía los progresos registrados en el diálogo EE.UU./UE sobre los datos del PNR, pero consideraba "que estos progresos no permiten concluir que se ha alcanzado un nivel adecuado de protección de los datos". Planteaba además que las mejoras debían dirigirse, entre otras cuestiones, a entender que "la finalidad de la transferencia de datos debe ser únicamente la lucha contra los actos de terrorismo y determinados delitos conexos que habrá

[711] Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp87_es.pdf

que definir; la lista de los datos que deben transferirse debe ser proporcionada y no excesiva; los datos sensibles no deben transmitirse; debe facilitarse a los pasajeros información clara, actual y comprensible; deben preverse disposiciones suficientes que garanticen a los pasajeros el acceso a un mecanismo de recurso verdaderamente independiente; debe establecerse un método de transferencia "push", es decir, que los datos sean seleccionados y transferidos por las compañías aéreas a las autoridades estadounidenses".

El Parlamento, por su parte, continuó oponiéndose a la actuación de la Comisión, y siguiendo la línea argumental que para ello había definido un informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE)[712], acordó con fecha 21 de abril de 2004, solicitar el dictamen del Tribunal de Justicia de la Unión Europea[713].

A pesar de esta situación tan tensa, la Comisión decidió emitir una Decisión sobre la adecuación de las transferencias de datos considerando, en coherencia con sus propósitos[714], que el Servicio de Aduanas y Protección de Fronteras de los Estados Unidos (CBP) si garantizaba una adecuada protección de los datos PNR transferidos por la Comunidad sobre los vuelos con destino o procedentes de los Estados Unidos, y el Consejo de Ministros, a su vez, emitió su decisión de aprobar un nuevo acuerdo sobre datos de pasajeros entre la Unión Europea y los Estados Unidos[715], que se firmaría en Washington el 28 de mayo de 2004[716].

---

[712] MANNY, C. *"La intimidad de la Unión Europea y la Seguridad de los Estados Unidos : la tensión entre la ley europea de protección de datos y los esfuerzos por parte de los Estados Unidos por utilizar los datos sobre pasajeros aéreos para luchar contra el terrorismo y otros delitos". Cuadernos de Derecho Público*, Nº 19-20. 2003. (Ejemplar dedicado a: Protección de datos). p.173.

[713] European Parliament Votes to Go to Court on EU-US PNR Deal. Disponible en: http://www.statewatch.org/news/2004/apr/13ep-vote-pnr-court.htm

[714] Decisión de la Comisión de 14 de mayo de 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (Bureau of Customs and Border Protection). Diario Oficial de la Unión Europea (6.7.2004) L 235/11 Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:235:0011:0022:ES:PDF

[715] Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection *(2004/496/EC).* Disponible en: http://www.statewatch.org/news/2004/mar/eu-us-pnr.pdf

[716] Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf

El Parlamento siempre sostuvo que la finalidad del registro de datos de pasajeros, debía guiarse por directrices generales e protección de la seguridad pública, y que por este motivo, aunque los datos provenían de una actividad económica privada, la de las compañías aéreas, no podía encuadrarse dentro del ámbito del derecho comunitario. La Comisión por su parte, entendía que esta actividad podía ser perfectamente amparada por la Directiva 95/46/CE[717].

El Tribunal de Justicia de la Unión Europea, en su Sentencia[718] de 30 de mayo de 2006, solucionó este conflicto, anulando la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos[719] y, la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos[720]. Estimó efectivamente que las Decisiones de la Comisión sobre los tratamientos de datos PNR, implican la transferencia de datos a terceros países (y no se centran sólo en tratamientos de carácter privado por las compañías aéreas[721]), y que por tanto no pueden amparase sin más en la Directiva 95/46/CE[722].

---

[717] GUERRERO PICÓ, C. "Operadores privados y seguridad pública: la retención de los datos de tráfico a la luz de la "sentencia PNR". *Revista de Protección de Datos*. Ed. Thomson Civitas. Junio 2007. Madrid p. 198.

[718] Disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2006/notas_prensa/common/C-0317_2004_ES_ARR.pdf

[719] Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0535:ES:HTML

[720] Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:183:0083:0083:ES:PDF

[721] Considerando 57 de la Sentencia: "Si bien es correcto considerar que los datos de los PNR son inicialmente recogidos por las compañías aéreas en el marco de una actividad comprendida en el ámbito de aplicación del Derecho comunitario, a saber, la venta de un billete de avión que da derecho a una prestación de servicios, sin embargo, el tratamiento de datos contemplado en la Decisión sobre el carácter adecuado de la protección tiene una naturaleza bien distinta. En efecto, como se ha recordado en el apartado 55 de la presente sentencia, el tratamiento de datos a que se refiere esta Decisión no es necesario para la realización de una prestación de servicios, sino que se considera necesario para salvaguardar la seguridad pública y para fines represivos".

[722] Considerando 63 de la Sentencia: "Afirma que esta Decisión no tiene por objeto y contenido el establecimiento y el funcionamiento del mercado interior, contribuyendo a la eliminación de obstáculos a la libre prestación de servicios, y no contiene disposiciones que persigan la consecución de este objetivo.

Tras esta Sentencia, el 27 de junio de 2006, el Consejo autorizó a la Comisión a entablar nuevas negociaciones para llegar a otro acuerdo con Estados Unidos, considerando que si ofrecían un nivel adecuado de protección de los datos del PNR que se transfieren desde la Unión Europea.

El resultado de estas negociaciones se plasmó en la Decisión 2006/729/PESC/JAI del Consejo, de 16 de octubre de 2006, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional (Department of Homeland Security) de los Estados Unidos[723], reconociendo la "importancia que revisten la prevención y la lucha contra el terrorismo, los delitos afines y otros delitos graves de carácter transnacional, incluida la delincuencia organizada, al tiempo que se respetan los derechos y las libertades fundamentales, especialmente la intimidad y, en todo caso, teniendo en cuenta el artículo 6, apartado 2, del Tratado de la Unión Europea sobre el respeto de los derechos fundamentales y, en particular, el derecho conexo relativo a la protección de los datos personales, y los compromisos publicados el 11 de mayo de 2004 por el DHS, el Servicio de Aduanas y Protección de Fronteras (Bureau of Customs and Border Protection)".

Una vez hubo expirado la vigencia de esa decisión (el 31 de julio de 2007) se dictó una nueva en la misma línea: la Decisión 2007/551/PESC/JAI del Consejo, de 23 de julio de 2007, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de

---

En efecto, su finalidad consiste en legalizar el tratamiento de datos personales impuesto por la legislación de Estados Unidos. Además, el artículo 95 CE no puede constituir la base de la competencia de la Comunidad para celebrar el Acuerdo, dado que éste se refiere a tratamientos de datos que no están comprendidos en el ámbito de aplicación de la Directiva".
Considerando 67 de la Sentencia: "El artículo 95 CE en relación con el artículo 25 de la Directiva no puede constituir la base de la competencia de la Comunidad para celebrar el Acuerdo.
Considerando 68 de la Sentencia: En efecto, el Acuerdo se refiere a la misma transferencia de datos que la Decisión sobre el carácter adecuado de la protección y, por tanto, a tratamientos de datos que, como ya se ha expuesto anteriormente, no están comprendidos en el ámbito de aplicación de la Directiva".
Considerando 69 de la Sentencia: "Por consiguiente, la Decisión 2004/496 no pudo adoptarse válidamente sobre la base del artículo 95 CE".

[723] Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:298:0027:01:ES:HTML

nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007) - Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007)[724]. Esta decisión, aplicable durante siete años, exige que las partes garanticen el respeto de los derechos y las libertades fundamentales de los pasajeros y, obliga a las compañías aéreas a transmitir al DHS (Departamento de Seguridad del Territorio Nacional de los Estados Unidos) los datos de los pasajeros con destino o salida de los Estados Unidos, con el compromiso de que éste garantizará un elevado nivel de protección. Además, en su texto, como Anexo, incluía una carta de acompañamiento del DHS, enviada a la Comisión con "el fin de reiterar la importancia que el Gobierno de los Estados Unidos concede a la protección de la intimidad de las personas", y con el objeto explicar los principios que aplica el DHS a la hora de recopilar, utilizar y almacenar datos de los registros de nombres de pasajeros (PNR): "presenta las garantías establecidas en la legislación estadounidense y refleja las normas de actuación que el DHS aplica, con arreglo a dicha legislación, a los datos de PNR derivados de vuelos entre los EE.UU. y la Unión Europea" (en lo sucesivo, "los datos de PNR de la UE").

Esta decisión recoge, en esencia, las siguientes cuestiones y compromisos por parte de Estados Unidos:

1.- Objeto para el cual se utiliza el PNR: "prevenir y combatir el terrorismo y los delitos afines, otros delitos graves de carácter transnacional, incluida la delincuencia organizada, y la huida de las personas objeto de órdenes judiciales o penas de prisión por alguno de los mencionados delitos".

2.- Uso compartido del PNR: Se tratarán los datos de PNR de la UE por el DHS de conformidad con la legislación estadounidense, como datos

[724] Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:01:ES:HTML

sensibles y confidenciales que se proporcionan sólo a autoridades estatales internas con competencias "en materia policial y judicial, de seguridad pública o antiterrorista, para ayudarlas en casos de lucha antiterrorista, delincuencia transnacional y seguridad pública" (…), y solo se entregarán a autoridades estatales de terceros países si se consideran adecuados los fines para los que quieran emplearse dichos datos y si se considera que tienen medios suficientes para protegerlos.

3.- Tipo de información recopilada: "Código del localizador de registro de nombres de los pasajeros; fecha de reserva/emisión del billete; fecha o fechas de viaje previstas; nombre o nombres de los interesados; información disponible sobre viajeros frecuentes y ventajas correspondientes (billetes gratuitos, paso a la categoría superior, etc.); otros nombres recogidos en el PNR, incluido el número de viajeros del PNR; toda la información de contacto disponible (incluida la información del expedidor); todos los datos de pago/facturación disponibles (excluidos los demás detalles de la transacción relacionados con una tarjeta de crédito o una cuenta y no relacionados con la transacción correspondiente al viaje); itinerario de viaje para ciertos datos de PNR; agencia/agente de viaje; Información sobre códigos compartidos; información escindida/dividida; situación de vuelo del viajero (incluidas confirmaciones y paso por el mostrador de facturación en el aeropuerto); información sobre el billete, incluidos el número del billete, los billetes de ida solo y la indicación de la tarifa de los billetes electrónicos (Automatic Ticket Fare Quote, ATFQ); toda la información relativa al equipaje; datos del asiento, incluido el número; observaciones generales, incluida la información sobre otros servicios (OSI), información sobre servicios especiales (SSI) y sobre servicios especiales solicitados (SSR); cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API), y todo el historial de cambios de los datos de PNR indicados en los números 1 a 18".[725]

[725] Continúa: "Estas medidas pueden consultarse en el sitio web del DHS www.dhs.gov. Cuando los datos de PNR de la UE mencionados incluyen datos sensibles (es decir, datos personales que indiquen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a un sindicato o el estado de salud o la vida sexual del viajero), según lo especificado en los términos y códigos PNR determinados por el DHS en consulta con la Comisión Europea, el DHS emplea un sistema automatizado que filtra esos términos y códigos PNR sensibles y no utiliza dicha información. A menos que se acceda a los datos para un caso excepcional, según se define en el párrafo siguiente, el DHS suprime sin demora los datos de PNR de la UE de carácter sensible. En supuestos de necesidad ante un

4.- Acceso y medios de recurso: Los particulares que necesiten información o corregir sus datos de PNR, podrán recurrir las decisiones a través de un sistema específico previsto al efecto por el DHS, con independencia de su nacionalidad o país de residencia[726].

5.- Notificaciones: Asimismo, el DHS publica información útil sobre estas cuestiones tanto para las compañías aéreas como para los viajeros, a través de su página web[727].

6.- Conservación de datos: "El DHS conserva los datos de PNR de la UE en una base de datos analítica activa durante siete años"; pasado este plazo los datos pasan a una situación no operativa, siendo conservados durante otros ocho años más, y sólo se podría acceder a ellos con la autorización de un agente de alto nivel del DHS designado por el Secretario de Seguridad del Territorio Nacional y, únicamente, "en respuesta a una situación, amenaza o riesgo identificable"[728]. Los datos relacionados con

---

caso excepcional que ponga en peligro la vida o la integridad física del titular de los datos o de otras personas, los agentes del DHS pueden necesitar y emplear datos de PNR de la UE distintos de los enumerados supra, incluidos datos sensibles. En tales casos, el DHS llevará un registro de acceso a todos los datos sensibles de los PNR de la UE y los suprimirá en un plazo máximo de 30 días a partir del momento en que se haya alcanzado el objetivo para el cual se accedió a ellos, siempre que su conservación no esté prescrita por ley. El DHS notificará a la Comisión Europea (Dirección General de Justicia, Libertad y Seguridad), normalmente en un plazo de 48 horas, que ha accedido a tales datos, incluidos datos sensibles".

[726] Continúa: "Por otra parte, los datos de PNR facilitados por un particular o por un tercero en su nombre se revelarán al particular de conformidad con las Leyes estadounidenses de protección de la intimidad y de libertad de la información. La Ley de libertad de la información (Freedom of Information Act, FOIA) permite a cualquier ciudadano (con independencia de su nacionalidad o país de residencia) acceder a los registros de una agencia federal de los EE.UU., salvo en caso de que dichos registros (o parte de ellos) no puedan revelarse en virtud de una exención prevista en dicha Ley. El DHS solo comunica los datos de PNR a los titulares de los datos o a sus agentes, de conformidad con la legislación estadounidense. Las solicitudes de acceso a información personalmente identificable contenida en el PNR que haya sido facilitada por el solicitante pueden remitirse a la siguiente dirección: FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 [tel. (202) 344-1850, fax (202) 344-2791]. En ciertas circunstancias de carácter excepcional, el DHS puede acogerse a las atribuciones que le reconoce la Ley de libertad de la información para denegar o posponer la comunicación de la totalidad o una parte de los datos de PNR a un solicitante que sea el propio titular de los datos, en virtud del título 5, artículo 552.b), del Código de los EE.UU. Con arreglo a la Ley de libertad de la información, cualquier solicitante está facultado para impugnar administrativa y judicialmente la decisión del DHS de no divulgar información".

[727] Véase el anterior Dictamen 2/2007 relativo a la información de los pasajeros en relación con la transferencia de datos PNR a las autoridades de los Estados Unidos, de 15 de Febrero de 2007, y posterior, su revisión de 24 de Junio de 2008. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp132_es.pdf

[728] Continúa: "Esperamos que los datos de PNR de la UE se supriman al final de este período; el DHS y la UE tratarán las cuestiones relacionadas con la conveniencia y el momento de la destrucción de los datos de PNR recopilados de conformidad con la presente carta en el marco de ulteriores negociaciones (…). El DHS tiene intención de analizar el efecto de estas normas de conservación en las operaciones e investigaciones a la luz de la experiencia que se adquiera en los próximos siete años. El DHS examinará con la UE los resultados de dicho análisis".

casos o investigaciones específicos podrían conservarse en la base de datos activa hasta que se hubiese archivado el caso o la investigación.

7.- Transmisión: Se pretende con el tiempo, pasar a un sistema de transmisión ágil y eficaz, para que sean las propias compañías aéreas que operen vuelos entre la UE y EEUU las que remitan los datos PNR a las autoridades[729].

8.- Reciprocidad: "el DHS entiende que no se le está pidiendo que adopte para su sistema PNR medidas de protección de datos más restrictivas que las que las autoridades europeas aplican a sus propios sistemas PNR nacionales", ni viceversa.

Tras la puesta en marcha de estos compromisos, parte de la Comisión Europea la siguiente iniciativa de mejora de las condiciones de este tipo de tratamiento de datos. El Consejo, con fecha 6 de noviembre de 2007, emitió una propuesta de decisión marco[730] sobre la utilización de datos del registro de nombres de los pasajeros (Passenger Name Record - PNR) con fines represivos[731], a la que los Estados miembros deberían conformarse, a más tardar, el 31 de diciembre de 2010.

El Grupo de Trabajo del Artículo 29 se pronunció una vez más sobre las intenciones de la Comisión, y en esta ocasión además lo hizo de forma conjunta con el Grupo de Trabajo sobre Policía y Justicia, en un Dictamen[732] que criticaba duramente tanto el sistema como los hipotéticos resultados: "Si se ejecuta la versión actual del proyecto de Decisión marco, Europa daría

---

729 Continúa: "Al ejercer su facultad de apreciación a este respecto, el DHS actuará con sensatez y mesura".

730 Señala expresamente la propuesta, "que surge a raíz de los atentados de Madrid, el Consejo Europeo de los días 25 y 26 de marzo de 2004 invitó a la Comisión a presentar una propuesta que permitiera a la UE dotarse de un enfoque común en relación con la utilización de los datos de los pasajeros con fines represivos. Esta propuesta completa la Directiva 2004/82/CE del Consejo sobre la obligación de las compañías aéreas de comunicar los datos de las personas transportadas".

731 Disponible en: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14584_es.htm

732 Dictamen conjunto sobre la propuesta de Decisión marco del Consejo relativa al uso del registro de nombres de los pasajeros ("Passenger Name Record" - PNR) a efectos de la aplicación de la ley, presentado por la Comisión el 6 de noviembre de 2007. Adoptado el 5 de diciembre de 2007 por el Grupo de Trabajo del Artículo 29. Adoptado el 18 de diciembre de 2007 por el Grupo de Trabajo sobre Policía y Justicia.
Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145_es.pdf

un gran salto hacia una sociedad de plena vigilancia que convertiría a todos los viajeros en sospechosos. Como ya ocurrió en el caso de la conservación de los datos de tráfico (Directiva 2006/24/CE), entidades privadas recogerán una enorme cantidad de datos personales que almacenarán para un posible uso posterior por parte de organismos de la Administración pública, a pesar de que nunca se haya probado la eficacia y necesidad de dicho sistema. La recogida de datos afecta a todos los viajeros tanto si son sospechosos como si son, en la mayoría de los casos, ciudadanos inocentes, y permite la reconstrucción de sus itinerarios de viaje durante muchos años. Por estas razones, siguen existiendo dudas fundadas sobre si el planteamiento elegido por la UE de poner a todos los viajeros bajo vigilancia general y considerarlos sospechosos en la lucha contra el terrorismo y la delincuencia organizada es la manera correcta de abordar estos fenómenos". Aunque también reconoce que esta propuesta tiene un enfoque "más mesurado que el Acuerdo que le precede, porque se han especificado los fines limitándolos a la prevención y lucha contra el terrorismo y la delincuencia organizada".

A pesar de esto, hasta el año 2010 no se retoma el debate[733], con ocasión de la "Comunicación de la Comisión Europea, sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros a terceros países", emitida el 2 de Septiembre de 2010. Sobre ella, tanto el Supervisor Europeo de Protección de Datos, como el Grupo de Trabajo del Artículo 29, también opinaron duramente.

El Grupo de Trabajo del Artículo 29 ha cuestionado[734] la necesidad de "elaborar perfiles a gran escala para perseguir delitos relacionados con el terrorismo o la delincuencia transnacional basándose en los datos de los pasajeros. Señala que la Comisión Europea aún no ha presentado pruebas objetivas ni estadísticas de que los datos del PNR sean útiles para la lucha contra el terrorismo o la delincuencia transnacional. Aunque también

[733] Algunos documentos de trabajo intermedios: Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes. 2009. Disponible en: http://www.statewatch.org/news/2009/apr/eu-pnr-council-5618-rev1-09.pdf ; *PNR: Opinion of the Fundamental Rights Agency. 2008.* Disponible en: http://www.statewatch.org/news/2008/oct/ep-pnr-opinion-fra.pdf

[734] Dictamen 7/2010 relativo a la Comunicación de la Comisión Europea sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a terceros países. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp178_es.pdf

reconoce que se definen normas y criterios comunes que deben formar parte de cualquier acuerdo con países no miembros de la Unión Europea relacionado con el intercambio de datos PNR", y lo considera un paso positivo, "ya que su aplicación debería conducir en un principio a la obtención de un mayor nivel de protección de los datos para el ciudadano europeo". Asimismo se hace incapié en el respeto a la finalidad de los tratamientos de estos datos, y a que "ninguna otra autoridad gubernamental del país receptor puede utilizar los datos recogidos para ningún fin Comunicado de prensa que no esté relacionado con la lucha contra el terrorismo o la delincuencia transnacional grave".

Por su parte, el Supervisor Europeo de Protección de Datos[735], en principio celebra que exista una propuesta mejorada en esta materia, por constituir "un paso fundamental hacia el establecimiento de un marco general para el intercambio de datos PNR", pero advierte que "los sistemas PNR presentados en la Comunicación, no cumplen por sí mismos los controles de necesidad y de proporcionalidad". En particular, señala tener una especial preocupación, en relación con la utilización de los sistemas PNR para llevar a cabo la evaluación del riesgo o la elaboración de perfiles delictivos. Entiende que el desarrollo de normativas asociadas a los datos PNR debe tener en cuenta el marco general de protección de datos de la UE, y "resulta fundamental que todos los acuerdos con terceros países tengan en cuenta las nuevas exigencias de protección de datos que se están desarrollando en el marco institucional post-Lisboa". Asimismo, recuerda que "deben aplicarse condiciones más estrictas, en especial respecto del tratamiento de datos de carácter sensible, el principio de limitación a una finalidad específica, las condiciones de transferencias posteriores y la conservación de los datos. Para concluir, el SEPD insistía en el hecho de que todo acuerdo debe establecer la aplicabilidad directa de los derechos de los titulares de los datos", dado que la eficacia de los procedimientos de aplicación, tanto por parte de los titulares de datos como de las autoridades

[735] Dictamen del Supervisor Europeo de Protección de Datos relativo a la Comunicación de la Comisión sobre el enfoque global de las transferencias de Datos de Registro de Pasajeros (PNR, en inglés) a terceros países. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:357:0007:0011:ES:PDF

de supervisión, es una condición esencial para evaluar la idoneidad de cualquier acuerdo.

Por último, en febrero de 2011, la Comisión Europea ha presentado una propuesta de "Directiva sobre un registro de nombres de los pasajeros (PNR) de la UE destinada a combatir las formas graves de delincuencia y el terrorismo[736]: (…) Los Estados miembros analizarán y conservarán los datos a fin de prevenir, detectar, investigar y perseguir las formas graves de delincuencia y los actos de terrorismo".

La Comisión propone que las compañías aéreas transfieran los datos sobre los pasajeros de los vuelos internacionales (datos de las reservas), a una unidad específica del Estado miembro de llegada o de salida del vuelo. Además, insiste en que es imprescindible que los datos PNR no puedan ser utilizados para una finalidad "que no sea combatir las formas graves de delincuencia y los actos de terrorismo". Las autoridades, en ejercicio de sus funciones coercitivas, delegadas por los Estados miembros, "deberán hacer anónimos los datos un mes después del vuelo, y los datos no deberán conservarse más de cinco años en total (breve período de retención)". Además, habrán de preverse normas claras sobre "el modo de efectuar la transferencia de datos, por ejemplo del número de veces que las compañías aéreas podrán transferir los datos a los Estados miembros y la seguridad de dichas transferencias, a fin de limitar el impacto en la privacidad y minimizar los costes de las compañías aéreas".

Asimismo, introduce cierta claridad en las condiciones de ejercicio de los derechos de los pasajeros de recibir información exacta sobre la recogida de sus datos, de acceder a ellos, rectificarlos y eliminarlos, así como los derechos de indemnización y recurso judicial. Por otra parte, también tiene en cuenta que "los datos sensibles que puedan revelar el origen étnico o racial, las opiniones políticas o las creencias religiosas nunca podrán ser transferidos por las compañías aéreas, ni ser utilizados en modo alguno por los Estados miembros, quienes no podrán acceder a las bases de

[736] Nota de Prensa disponible en: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/120&format=HTML&aged=0&language=ES&guiLanguage=en

datos de las compañías aérea (los datos deberán ser solicitados y enviados a ellos por las compañías aéreas de que se trate)".

La propuesta considera que, en definitiva, la responsabilidad última de la seguridad de los datos tratados, es de los Estados miembros, y que por ello, deben "crear unidades específicas que manejen los datos y mantengan su seguridad" que a su vez sean supervisadas por una autoridad (de protección de datos) independiente. Se espera que las negociaciones duren dos años.

5. Escáneres de protección en los aeropuertos.

Después del intento frustrado de ataque terrorista con explosivos ocultos, en el vuelo 253 de Northwest Airlines, entre Amsterdam y Detroit (Estados Unidos), el 25 de diciembre de 2009, la influencia de Estados Unidos y sus políticas de seguridad estatal llevó a que, en Europa, Holanda fuese el primer país en implantar, en el aeropuerto de Schiphol, el uso de los escáneres corporales[737], seguido en esta iniciativa por Reino Unido (en Heathrow y Manchester[738]), e Italia en el aeropuerto de Fiumicino[739].

Esta tecnología consiste en un dispositivo de uso policial para el cacheo e inspección de los pasajeros mediante ondas milimétricas que proyectan una imagen muy definida del cuerpo humano, permitiendo la detección de cualquier material distinto de la piel humana. Pero desde el principio ha tenido en su contra un arduo debate sobre si respeta los

[737] Noticia de El Pais (30/1/2009).
http://www.elpais.com/articulo/internacional/Holanda/impone/escaner/corporal/vuelos/EE/UU/elpepuint/20091230elpepuint_7/Tes
[738] Ibídem (1/2/2010).
http://www.elpais.com/articulo/internacional/aeropuertos/britanicos/Heathrow/Manchester/incorporan/escaneres/corporales/elpepuint/20100201elpepuint_14/Tes
[739] Ibídem (4/3/2010).
http://www.elpais.com/articulo/internacional/Italia/estrena/escaner/corporal/aeropuertos/Roma/elpepuint/20100304elpepuint_12/Tes

derechos fundamentales, por cuanto los escáneres permiten visionar el cuerpo humano como si estuviera desnudo, y además, parecen vulnerar principios básicos en materia de salud pública, por cuanto emiten dosis de radiaciones ionizantes (rayos X) perjudiciales, cuestiones estas por las que ni siquiera en Estados Unidos, impulsor de este tipo de medidas de protección en los aeropuertos, a través de la Agencia de Seguridad del Trasporte (TSA), ha llegado a generalizar totalmente su uso.

A estas dos polémicas consideraciones, se sumó la desprotección de los datos obtenidos, después de que el portal web "Gizmodo" filtrase en noviembre de 2010[740] las imágenes de cientos de personas que habían sido sometidas a este tipo de control, evidenciando la falta de garantías en el almacenamiento y custodia de las imágenes que revelan los escáneres y, el perjuicio que ello podría suponer para los afectados.

Sobre este escenario, tanto la necesidad una normativa armonizada de carácter internacional, como la posibilidad de utilizar sistemas menos invasivos[741], habían impedido que se implantase su uso en los aeropuertos.

En Europa, en el marco de la política de protección de la aviación[742], se debía garantizar un enfoque armonizado del uso de los escáneres de protección en los aeropuertos, que fuera además respetuoso con el ejercicio de los derechos fundamentales reconocidos en la Carta de Derechos Fundamentales.

---

[740] Noticia de El Pais (17/11/2010) http://www.elpais.com/articulo/internacional/Filtradas/imagenes/ciudadanos/desnudos/escaneres/seguridad/EE/UU/elpepuint/20101117elpepuint_7/Tes

[741] Aeropuertos de EU, con escáneres menos reveladores: "la Agencia de Seguridad del Transporte (TSA) anunció este miércoles que instalará un nuevo sistema de detección menos impúdico. Este nuevo equipo "concebido para proteger mejor la vida privada será capaz de detectar objetos potencialmente peligrosos a partir de una silueta genérica para todos los pasajeros" *(…).* Noticia de El Economista. México. (20/07/2011) http://eleconomista.com.mx/internacional/2011/07/20/aeropuertos-eu-escaneres-menos-reveladores

[742] Con el fin de proteger el transporte por aire de personas y mercancías, la Unión Europea (UE) ha establecido una serie de normas comunes aplicables en todo el territorio comunitario para proteger la aviación civil de actos de interferencia ilícitos. El Reglamento (CE) nº 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) nº 2320/2002, establece normas comunes a toda la Unión Europea (UE) para proteger la aviación civil de actos ilícitos de interferencia. Las disposiciones del Reglamento contemplan todos los aeropuertos y partes de aeropuertos establecidos en un país de la UE y que no se utilicen exclusivamente para fines militares. Las disposiciones también se aplican a todos los operadores, incluidas las compañías aéreas que presten servicios en tales aeropuertos. También es de aplicación para toda entidad situada dentro o fuera de las instalaciones de los aeropuertos y que preste servicios a los mismos.

En el año 2008 la Comisión propuso al Consejo y al Parlamento Europeo, el 5 de septiembre, un proyecto de reglamento con una serie de requisitos básicos de control que facilitaban una lista de métodos y tecnologías de control reconocidos, incluidos los escáneres de protección, y el Parlamento Europeo adoptó una resolución[743] sobre el impacto de las medidas de seguridad de la aviación y los escáneres corporales en los derechos humanos, la privacidad, la dignidad personal y la protección de datos, solicitando una evaluación más detallada de la situación. La Comisión acordó revisar más a fondo estas cuestiones y retiró los escáneres de protección de su propuesta legislativa original. El proyecto legislativo se convirtió en el Reglamento (CE) nº 272/2009 de la Comisión[744].

El Supervisor Europeo de Protección de Datos, el Grupo de Trabajo del Artículo 29, y la Agencia Europea de los Derechos Fundamentales expresaron en 2009 sus reservas frente a los escáneres[745], por considerar que tenían un profundo impacto en la protección de la vida privada y de los datos personales de los pasajeros, y que "sólo podrían considerarse apropiados si su uso se adecuara a los requisitos de protección de datos y si se garantizasen los derechos de las personas en los aeropuertos".

En el año 2010, se pusieron en marcha los primeros ensayos con escáneres de protección como método de control de los pasajeros se realizaron en Finlandia, en el aeropuerto de Vantaa de Helsinki y, en el Reino Unido, en el aeropuerto londinense de Heathrow. El Supervisor Europeo de Protección de Datos[746] puso de manifiesto que existen otros modelos menos invasivos que los que se venían promocionando desde Estados Unidos.

---

[743] La Resolución (2008)0521 del Parlamento Europeo pedía a la Comisión que llevara a cabo "una evaluación del impacto sobre los derechos fundamentales, que consultara al Supervisor Europeo de Protección de Datos, al Grupo de trabajo del artículo 29 y a la Agencia Europea de los Derechos Fundamentales, que realizara una evaluación científica y médica sobre las posibles repercusiones de esas tecnologías en la salud y que efectuara una evaluación sobre el impacto económico y comercial y en términos de coste-beneficio".

[744] Reglamento (CE) nº 272/2009 de la Comisión, de 2 de abril de 2009, que completa las normas básicas comunes sobre la seguridad de la aviación civil establecidas en el anexo del Reglamento (CE) nº 300/2008 del Parlamento Europeo y del Consejo (DO L 91 de 3.4.2009, p. 7).

[745] Carta de 11.2.2009 que dirigiera el Presidente del Grupo de trabajo del artículo 29 a la Dirección General de Transportes, así como la consulta adjunta.

[746] Reacción del Supervisor en la reunión de la Comisión LIBE sobre la reciente evolución de las políticas antiterroristas (escáneres corporales, vuelo de Detroit). Parlamento Europeo, Bruselas, 27 de enero de 2010.

La Comisión Europea, en la "Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo, sobre el uso de escáneres de protección en los aeropuertos de la UE"[747], reconoce que, de conformidad con el Derecho de la UE, "los Estados miembros pueden introducir en sus aeropuertos el uso de escáneres de protección i) ejerciendo su derecho a aplicar medidas de seguridad más estrictas que los requisitos vigentes en el conjunto de la Unión o ii) ejerciendo de forma temporal –durante un período máximo de 30 meses– su derecho a realizar pruebas con nuevos métodos o procedimientos técnicos*"*[748]*.* Y expresamente señala que: "Todo el Derecho de la UE, incluida la normativa que regula la protección de la aviación y sus disposiciones de aplicación, debe respetar los derechos fundamentales y las normas sanitarias que la Unión ha establecido y protege".

Los derechos fundamentales a tener en cuenta, respecto del uso de este tipo de escáneres, reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea, son en concreto: "la dignidad humana (artículo 1), el respeto de la vida privada y familiar (artículo 7), la protección de los datos de carácter personal (artículo 8), la libertad de pensamiento, de conciencia y de religión (artículo 10), la no discriminación (artículo 21), los derechos del menor (artículo 24) y la garantía de un alto nivel de protección de la salud humana en la definición y ejecución de todas las políticas y acciones de la Unión (artículo 35)".

Es sorprendente que además reconozca la ineficacia de las tecnologías en el control de la seguridad, exponiendo que cada nuevo punto de control en los aeropuertos "se sobrecarga con la instalación de nuevos

[747] COMISIÓN EUROPEA. Bruselas, 15.6.2010. COM(2010) 311 final. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el uso de escáneres de protección en los aeropuertos de la UE, relativa a la seguridad de la aviación, proteger a las personas y las mercancías de actos de interferencia ilícitos a la aviación civil. Tras los ataques del 11 de septiembre de 2001, la UE estableció un marco de seguridad común de la aviación. Uno de sus elementos claves es que cada pasajero y cada equipaje o carga que salga de un aeropuerto de la UE deberá pasar el control de detección u otro control de seguridad que garantice que no se introduce ningún artículo prohibido en las áreas de seguridad restringidas de los aeropuertos ni a bordo de los aviones. Últimamente, la aviación civil se ha estado enfrentando a nuevos tipos de amenazas contra los que las tecnologías tradicionales de seguridad de los aeropuertos no son del todo efectivas, tal y como ocurrió recientemente con el intento de ataque terrorista del 25 de diciembre de 2009, en el que un pasajero ocultó explosivos en un vuelo de Ámsterdam a Detroit
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0311:ES:NOT

[748] La base jurídica de las pruebas es el capítulo 12.8, «Métodos de control con nuevas tecnologías», del anexo del Reglamento (UE) nº 185/2010 de la Comisión (antiguo artículo 4 del Reglamento (CE) nº 820/2008 de la Comisión).

equipos y la realización de nuevas tareas al servicio de la protección", abogando por sistemas de intercambio de información policial de análisis del factor humano (por ejemplo, la observación del comportamiento de los pasajeros) y, sin embargo, acepte que "los escáneres de protección pueden maximizar las posibilidades de detectar amenazas y ofrecernos una capacidad de prevención considerablemente mayor (basta con unos 20 segundos para producir e interpretar los datos pertinentes del pasajero). Es verdad que esa mayor eficacia de detección puede alcanzarse también con un registro manual completo. Sin embargo, este método se considera enojoso y no gusta por tanto ni a pasajeros ni a inspectores".

Respecto de la obligatoriedad de su uso, lo acepta como el sistema más recomendable, y dice que la posibilidad de negarse a este tipo de controles, debe venir dada "por motivos relacionados con la salud o con los derechos fundamentales cuando haya métodos alternativos que ofrezcan garantías de seguridad equivalente, porque si fuera estrictamente voluntario, se mitigaría considerablemente cualquier preocupación relacionada con los derechos fundamentales. Ahora bien, al barajar esta opción, debería quedar claro que los pasajeros que rechazasen sujetarse a esa tecnología tendrían que someterse –para mantener los altos niveles de protección de la aviación que son necesarios– a un método de detección alternativo de eficacia similar, como, por ejemplo, los registros manuales completos del cuerpo".

Centrándonos en la protección de los derechos fundamentales, la Comisión Europea precisa que las normas de funcionamiento, la elección de los pasajeros que deben ser analizados con un escáner corporal, "garanticen que los pasajeros a los que se pida pasar por un escáner de protección no se elijan en función de su género, raza, color, origen étnico o social, religión o creencia"[749]. Y que, en materia de protección de datos, "la inspección ha de

[749] Además, se concreta (p.13): "La capacidad que tienen algunas tecnologías de inspección para ofrecer una imagen detallada (aunque sea borrosa) del cuerpo humano y desvelar problemas médicos (detectando, por ejemplo, prótesis o pañales) ha sido censurada desde la perspectiva de la privacidad y de la dignidad humana. Hay, además, personas a las que puede resultar difícil reconciliar sus creencias religiosas con un procedimiento en el que la imagen de su cuerpo tenga que ser examinada por un inspector. Por otra parte, los derechos de la infancia y, entre ellos, el de protección y cuidado, así como el requisito de la Carta de Derechos Fundamentales que obliga a que en todas las políticas y actividades

respetar los criterios siguientes: i) que la medida propuesta sea adecuada para alcanzar el objetivo que se persiga (detectar objetos no metálicos y aumentar así el nivel de protección), ii) que la medida no vaya más allá de lo necesario para la consecución del objetivo y iii) que no haya ningún otro medio que resulte menos embarazoso*".* Por otra parte, recuerda que de conformidad con la Directiva 95/45/CE[750], las imágenes podrían utilizarse "únicamente para los fines de protección de la aviación, no debiendo ser posible, en principio, almacenar ni recuperar la imagen de una persona creada por un escáner una vez que ésta haya abandonado ya el punto de control por no habérsele encontrado ningún objeto o artículo que suponga una amenaza".

Esta comunicación, termina concluyendo que la existencia de unas normas comunes de la UE "para los escáneres de protección, puede garantizar la igualdad en la protección de los derechos fundamentales y de la salud. Ese nivel común de protección de los ciudadanos europeos puede garantizarse con el establecimiento en la normativa de la Unión de unas normas técnicas y unas condiciones operativas que regulen el uso de los escáneres. La aplicación uniforme de esas normas y condiciones en todos los aeropuertos de la UE sólo puede garantizarse legalmente si el enfoque es el mismo en toda la Unión. Tal enfoque es esencial para garantizar tanto el más alto nivel de protección de la aviación, como la máxima protección posible de los derechos fundamentales y la salud de los ciudadanos europeos*".*

Pero entiende que, aunque "los Estados miembros están facultados para instalar escáneres de protección, bien para someterlos a prueba en los aeropuertos (Reglamento (CE) nº 185/2010 de la Comisión: Finlandia, Francia, los Países Bajos, Italia y el Reino Unido han introducido ya escáneres de protección en virtud de la normativa vigente de la UE) o bien

europeas se garantice un alto nivel de salud pública, exigen aquí un cuidadoso análisis de todos los aspectos tocantes a los niños".

[750] La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, "dispone que la persona de la que vayan a tomarse imágenes (como lo hace la tecnología de algunos escáneres de protección) sea informada previamente de que va a ser objeto de esa medida y de posible uso de sus imágenes. La norma es que los datos personales, como lo son las imágenes, sólo se recojan, procesen y utilicen de acuerdo con los principios aplicables en materia de protección de datos".

como medida de protección", la normativa de ese momento no permitía que los aeropuertos sustituyeran sistemáticamente los métodos o tecnologías de inspección "tradicionales" por escáneres de protección, ya que para que "esos escáneres pudieran autorizarse como un método más de protección de la aviación, sería necesaria una decisión de la Comisión apoyada por los Estados miembros y por el Parlamento Europeo, que modificara el Reglamento (CE) nº 272/2009 de la Comisión".

En el mes de mayo de 2011, la Comisión de Transporte del Parlamento Europeo aprobó las normas que deberían cumplir los escáneres corporales, basándose en un informe de iniciativa de Luis de Grandes Pascual (PPE, España), que fue aprobado por el pleno del Parlamento Europeo en el mes de Julio[751] entendiendo su normalización común "en toda la UE, y una vez que se haya demostrado que no ponen en riesgo la salud, la dignidad y la intimidad de los pasajeros y, que los viajeros tienen derecho a elegir métodos de control alternativos si así lo desean".

En noviembre de 2011, la Comisión Europea, aprobó reglamento que regulará el uso de escáneres corporales en los aeropuertos de los países miembros de la Unión Europea, entre cuyas medidas se encuentran: la obligación de que los pasajeros sean informados de las condiciones en que se realiza el control, y que puedan rechazar la exploración, ofreciéndose un método de control alternativo (manual). Los pasajeros también podrán elegir si desean que la imagen escaneada sea revisada por un hombre o una mujer. Las imágenes producidas por los escáneres no se podrán grabar o copiar, y no podrán estar vinculadas a datos de identificación del viajero. La imagen de la cara debe ser borrosa, y las personas que revisen las imágenes deberán estar en un lugar separado de los pasajeros para que no puedan ver sus caras[752]. A partir del año 2012, será analizada y estudiada la

[751] Nota de Prensa. Parlamento Europeo Oficina de Información en España. (6/7/2011). "La seguridad en los transportes constituye una de las máximas preocupaciones en la lucha contra el terrorismo", señaló Luis de Grandes en el debate celebrado anoche. "Los sistemas que se proponen no muestran el cuerpo humano, sino una figura estándar, un muñeco, una foto del pasajero tal y como va vestido o simplemente un 'ok' en verde cuando el pasajero pasa sin saltar la alarma", añadió.
http://www.europarl.es/view//Sala_de_Prensa/press-release/pr-2011/pr-2011-July/pr-2011-Jul-16.html

[752] Nota de Prensa. 15.11.2011. www.hablamosdeeuropa.es, iniciativa de la Secretaría de Estado para la Unión Europea que pretende comunicar Europa y crear un diálogo abierto y permanente con los ciudadanos.

viabilidad práctica de esta normativa, siguiendo las bases descritas sobre protección de derechos fundamentales (dignidad y protección de de datos personales), y protección de la salud.

6. "SWIFT".

La Sociedad para las Comunicaciones Financieras Interbancarias Mundiales (SWIFT, por sus siglas en inglés[753]), se convirtió en un objetivo del interés público, tras los atentados del 11 de septiembre de Nueva York, porque transmitió datos confidenciales sobre transacciones financieras a las autoridades policiales, a través de un programa que se puso en marcha junto con el Departamento del Tesoro (UST[754]) de Estados Unidos, el Programa de Seguimiento de la Financiación del Terrorismo (TFTP[755]).

SWIFT es un proveedor belga de servicios financieros, que gestiona prácticamente todos los negocios bancarios transfronterizos de Europa. Tiene su sede central en Bélgica, y sede de operaciones está en EEUU, aunque cuenta con oficinas en los principales centros financieros y mercados en desarrollo del mundo, y la polémica en Europa se abrió sobre las consideraciones legales que debía tener la aplicación del secreto bancario y la protección de datos de carácter personal, en la investigación de los atentados terroristas u otros crímenes de especial gravedad.

Tras el 11-S Estados Unidos había recurrido a datos de SWIFT de clientes bancarios de Europa en su lucha contra el terrorismo, y el 23 de junio de 2006, el New York Times reveló que SWIFT había colaborado supuestamente con los organismos de los Estados Unidos de forma sistemática, realizando transferencias masivas de mensajes que habían sido

---

http://www.hablamosdeeuropa.es/Paginas/Prensa/Noticias/noticia.aspx?id=4a6a657d-3d7c-411a-8f23-e75892322527

[753] Society for Worldwide Interbank Financial Telecommunication.

[754] United States Department of the Treasury.

[755] Terrorist Finance Tracking Program.

intercambiados entre las instituciones financieras de todo el mundo durante más de cuatro años, como una parte esencial de un programa secreto del gobierno para la vigilancia general de las transacciones financieras en el contexto de la política de seguridad estatal (TFTP), criticado por el alcance de las medidas adoptadas de forma excepcional, sin tener en cuenta los derechos y libertades fundamentales.

Esta actuación fue recogida por la Autoridad de Protección de Datos Belga, siendo investigada durante más de dos años.

En un primer dictamen y en base a la información disponible en ese momento, la APD belga (seguido de cerca por sus homólogos europeos) puso de manifiesto sus sospechas sobre el hecho de que SWIFT había podido violar de forma grave la Ley belga de protección de datos y la normativa europea aplicable, e inició un procedimiento de control e inspección sobre SWIFT, que a su vez, dio a este la oportunidad de realizar las alegaciones que consideró oportunas sobre su forma de actuar.

Finalmente, el 9 de diciembre de 2008 tras dos años de investigaciones, la APD belga cerró las investigaciones y adoptó su decisión, borrando toda duda sobre la falta de garantías para el ejercicio efectivo de cada individuo de sus derechos de dos años de investigaciones. Concluyó que nada confirmaba las sospechas de que SWIFT hubiese violado grave y reiteradamente la Ley, y que la empresa había actuado con prudencia, de manera que los datos solicitados a SWIFT por las autoridades norteamericanas, estaban debidamente protegidos ("a diferencia de las masas de datos que fueron recogidos y explotados de manera sistemática en algunos programas de vigilancia de otros")[756].

Específicamente señaló que SWIFT había colaborado correctamente y sin reservas en el establecimiento de los hechos, y que no sólo se había limitado al cumplimiento de la legislación vigente, sino que incluso había tomado una serie de medidas más allá de sus obligaciones legales, con la

[756] http://www.privacycommission.be/en/press_room/pers_bericht11.html

única intención de mejorar la prevención de ciertos riesgos y mejorar la protección de los datos personales que los procesos de la empresa, por ejemplo, con el establecimiento de un centro de operaciones en Suiza entre países europeos mensajes (que ya no serán transferidos a los EE.UU.); el nombramiento de un "Oficial de Privacidad" con tareas específicas; la formalización de procedimientos de seguimiento de las peticiones de las personas cuyos datos sean procesados; la creación de un grupo de trabajo permanente para la protección de datos, para evaluar y adaptar las medidas de seguridad existentes; el desarrollo de políticas de información accesible, etc. La APD belga declaró que SWIFT ofrecía las garantías exigidas por la Comisión Europea en materia de protección de datos, archivando el caso.

Con nueva sede en Suiza, EEUU había perdido parte de sus "privilegios" en el acceso a datos de SWIFT, y se hizo necesario un acuerdo para la transferencia internacional de este tipo de información.

En noviembre de 2009 los Ministros Europeos de Interior sellaron un acuerdo SWIFT, que sin embargo, no fue ratificado por el Parlamento Europeo, que según el Tratado de Lisboa debía ratificarlo.

Durante las negociaciones, se pusieron de manifiesto, en la Comisión de Libertades Civiles del Parlamento Europeo, diversas opiniones en contra del acuerdo de transferencia de datos financieros entre Europa y Estados Unidos. Los comisarios en general no estaban de acuerdo con el contenido de la propuesta de acuerdo, y así, la liberal holandesa Jeanine Hennis-Plasschaert, señaló que "con estas directrices seguimos hablando de transferencias de bloques de datos", lo que supondría "noventa millones de datos al mes", o el eurodiputado maltés del grupo del Partido Popular Europeo Simon Busuttil subrayó que "es importante que evitemos desde el principio las transferencias de datos a granel", mientras que la socialista alemana Birgit Sippel resaltó que "hasta los bancos más pequeños pueden tratar los datos de forma individualizada". También expresaron su preocupación ante asuntos como los derechos que tendrían los ciudadanos europeos a reclamar a las autoridades estadounidenses ante un hipotético

uso irregular de sus datos, o la posible falta de constitucionalidad del acuerdo en algunos Estados miembros[757].

Finalmente, el 27 de julio de 2010, fue publicado en el Diario Oficial de la Unión Europea, el Acuerdo SWIFT[758] a que llegaron la Comisión Europea y el Departamento del Tesoro de los Estados Unidos con fecha han firmado el 28 de junio 2010, para permitir al Departamento del Tesoro de Estados Unidos recibir datos del servicio de mensajería financiero almacenados en la UE, y así poder realizar actuaciones y tratamientos de datos personales bancarios en la lucha contra el terrorismo, "garantizando un nivel satisfactorio de protección de datos".

Pero, según la Agencia Española de Protección de Datos, junto con el resto de autoridades europeas, el acuerdo "TFTP II: Programa de Seguimiento de la Financiación del Terrorismo", conocido como Acuerdo Swift, y que tiene como finalidad la transparencia de datos sobre transacciones financieras desde la UE a Estados Unidos, supone por el contenido de varias de sus disposiciones, "riesgos graves para la protección de datos y debilitan los principios actuales de la UE sobre protección de datos personales", asimismo, consideran que "no se garantiza completamente el derecho a recurso judicial no discriminatorio en EE.UU, a los ciudadanos cuyos datos personales sean tratados en la UE", y ponen en duda si "las personas que no son ciudadanos de Estados Unidos van a tener derecho a la reparación judicial de sus derechos". Otra de las preocupaciones señaladas por las autoridades europeas son las transferencias de datos financieros que podrán administradas por las Fuerzas de Seguridad de ambas partes, pues tal y como se hallan establecidas, no cumplen las garantías exigidas por la legislación de la UE, especialmente lo relativo al período de conservación de los datos (cinco años como máximo) y "las autoridades europeas de protección de datos no van a

[757] Nota de prensa. Justicia y asuntos de interior (08-04-2010). http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20100406STO72100&language=ES

[758] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:195:0005:0014:EN:PDF

poder garantizar que los derechos de una persona se están respetando en todo momento".

Incluso señalan que: "Las autoridades europeas de protección de datos han decidido que, si el acuerdo entrase en vigor, intentarán por todos los medios que se incluya en la primera revisión conjunta la transferencia masiva y la transferencia ulterior de transacciones financieras. Además, también quiere asegurarse de que no se transfieren los datos internos europeos sobre transacciones financieras, lo que se denomina datos SEPA (Single European Payment Area), ya que el acuerdo es ambiguo en este sentido" [759].

[759] Nota de Prensa AEPD. (29.06.2010). https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/junio/100629_NP_OPINION_29_TFTP.pdf

V.- CONCLUSIONES: ESTADO DE DERECHO, SEGURIDAD Y PROTECCIÓN DE DATOS.

La Sentencia del Tribunal Constitucional alemán sobre la Ley del Censo de 1983, primera en Europa que definió el derecho fundamental a la protección de datos de carácter personal como el "derecho a la autodeterminación informativa". Era ya muy consciente de que en virtud de la "evolución de los condicionamientos tecnológicos, es posible producir una imagen total y pormenorizada de la persona respectiva - un perfil de la personalidad-, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en "hombre de cristal"[760], y por este motivo comprendía la necesidad de que los legisladores estatales regulasen cuidadosamente el uso de la tecnología en relación con las personas, y teniendo en cuenta que la posibilidad de acceso por parte del Estado a los datos de una persona, y su utilización posterior, debía ser valorado siempre en relación directa con el interés y derecho del individuo a permanecer anónimo o aislado[761].

[760] Ibídem. GRUNDE II.

[761] "Las posibilidades de la moderna elaboración de datos son reconocidamente inteligibles para personas especializadas y son susceptibles de suscitar en el ciudadano el temor a una aprehensión incontrolada de su personalidad, incluso en el caso de que el legislador se limitase a recabar unos datos indispensables razonablemente exigibles". Sentencia del Tribunal Constitucional Federal Alemán, sobre la Ley del Censo Alemana, de 15 de Diciembre de 1983. Boletín de Jurisprudencia Constitucional, Nº 33. Enero, 1984. GRUNDE. A.

En aquel momento, al Tribunal Constitucional alemán ya le preocupaba el hecho de que los ciudadanos no pudiera "percibir con seguridad suficiente que informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes", porque podrían verse cohibidos "en su libertad de planificar o decidir por autodeterminación". Es decir, reconoció que la tecnología tiene posibilidades ilimitadas para el tratamiento de datos de los individuos, y le preocupaba que pudieran producirse intervenciones demasiado inquisitivas, ya que podrían derivar en efectos tan perversos como llegar condicionar el comportamiento del ciudadano "hasta el punto en que no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos".

Sin embargo se reconocía también su utilidad, y que la capacidad de decisión de los ciudadanos sobre su propia información personal no podía considerarse en absoluto ilimitada. Se estimaba que era necesario un equilibrio en la ponderación de los intereses en juego en cada momento, debiendo ceder en no pocas ocasiones en favor de la protección de la comunidad.

Las dificultades de lograr ese equilibrio aún hoy continúan poniéndose de manifiesto. Cada situación exige o pretende nuevas necesidades de control en función de los nuevos peligros que puedan acechar a la comunidad y, por supuesto, en función de los intérpretes de los mismos. Es tan importante tener en cuenta el peligro, como su justa valoración, pues como ya se ha señalado, tan restrictivas pueden ser para el ciudadano aquellas medidas que permitan al Estado utilizar su información personal sin su conocimiento, como aquellas medidas que se le impongan con total transparencia, pues al fin y al cabo, en el primero de los casos, su libertad sería cercenada a posteriori, con el resultado de su vigilancia y, en el segundo de los casos, su libertad de comportamiento estaría siendo dirigida a priori.

PEREZ LUÑO lo explicó de un modo más visceral, señalaba que "en la sociedad tecnológica de nuestro tiempo los ciudadanos más sensibles a la defensa de los derechos fundamentales se sienten crispados o atemorizados porque advierten que las conquistas del progreso se ven contrapuntadas por graves amenazas para su libertad, su identidad e incluso su propia supervivencia. La ciencia y la tecnología han mantenido en los últimos años un ritmo de crecimiento exponencial, que no siempre ha tenido un puntual reflejo en la evolución de la conciencia ética de la humanidad. Por ello, las trampas liberticidas subyacentes en determinados empleos abusivos de la cibernética o de la informática, el peligro de la catástrofe ecológica, o la psicosis de angustia que genera la amenaza latente de un conflicto atómico, son el trasfondo terrible que amenaza el pleno ejercicio de los derechos fundamentales y acecha con invalidar los logros del progreso"[762].

La tecnología ha rediseñado las relaciones personales, sociales, políticas y económicas, y aunque no siempre ha sido para mejorarlas, el papel del Estado en su dominio ha sido decisivo. Pero, como se pregunta el profesor RODOTÁ: "¿bastará el refuerzo de las garantías institucionales para contrastar el impulso de las nuevas tecnologías hacia la creación de una sociedad de vigilancia y clasificación? Preocupa ver cómo se ha ido produciendo una convergencia de intereses, públicos y privados, que ha acelerado la construcción de una sociedad de vigilancia, con controles cada vez más intensos en cada espacio y de una sociedad de clasificación, con una transformación de cada espacio en un lugar donde impera la lógica comercial. Este nuevo contexto no evoca el 'Gran Hermano' de GEORGE ORWELL, sino el 'Panopticón' de Jeremy Bentham, donde hay muchos sujetos públicos y privados que pueden ver todos sin ser vistos. Nace un control asimétrico que puede ser peligroso para los derechos de los ciudadanos". [763]

El control desmedido al que estamos siendo sometidos hoy por hoy, y cuya inicial intención podría considerarse completamente legítima, ha

[762] PÉREZ LUÑO, A.E. Los derechos fundamentales (6ª ed.), Col. Temas Clave de la Constitución Española. Madrid, 1995. p.28.
[763] RODOTÁ, S. "Tecnología y Derechos Fundamentales". *Datospersonales.org*. Revista De la Agencia Española de Protección de Datos de la Comunidad de Madrid, nº 8. Madrid, 2004.

llegado a configurar una sociedad en la que todos somos sospechosos, en que "la protección de los datos personales se presenta como una precondición por la actuación de estos derechos 'viejos' y como elemento básico de los derechos 'nuevos' en la edad de la tecnología", hasta el punto en que nuestro propio cuerpo pasa a ser fuente de información (un *password*): "la ciudadanía electrónica".

Este tipo de ciudadanos acepta sin más ser escudriñados por el Estado, siempre bajo la convicción o influidos por un factor esencial: la seguridad, y lo hacen sin entrar a valorar en qué medida pueda verse limitada su espontaneidad o su libertad.

El criptógrafo BRUCE SCHNEIER, ha ilustrado los efectos del sentimiento de desprotección en el comportamiento humano y en su psicología[764]. En su artículo "La psicología de la seguridad" expone conclusiones tales como que observar las circunstancias sociales existentes al momento de adoptar una serie de medidas de seguridad para la comunidad, es tan importante como la percepción que tengan del riesgo los individuos en ese mismo momento. Explica que una toma de decisiones eficiente en materia de seguridad dependerá de si existe o no una gran divergencia entre la realidad del momento y la percepción de esa realidad por los individuos, es decir, que la protección eficiente dependerá de la correcta percepción de los riesgos. Así, cuando esa percepción sea inexacta, ya se infravalore, ya se exagere, las medidas de seguridad que se adopten bajo eso parámetros no van a tener resultados óptimos, no va a ser posible aplicarlas a la realidad de manera eficiente, repercutiendo de forma negativa en los destinatarios de dichas medidas.

En términos de utilidad, la expectativa de los beneficios que se pueden obtener de una serie de medidas de seguridad, ha de ser puesta en relación directa con los perjuicios que van a resultar de la misma, buscando siempre un nivel óptimo o asumible de riesgo.

[764] SCHNEIER B. *The Psychology of Security*. 18 de enero de 2008. http://www.schneier.com/essay-155.html

Pero se tiende a manipular estas percepciones, los Estados buscan dirigir el sentimiento de los ciudadanos con el único fin de obtener concesiones y acceso a determinadas parcelas de sus vidas. Se procura que la gente simplemente se sienta más segura, aunque en realidad no lo esté. Es lo que SCHNEIER denomina como "El teatro de la seguridad"[765].

La psicología humana tiende a buscar la protección como una necesidad primaria, porque el sentimiento de seguridad aparentemente da paso a un sistema de vida y de convivencia en libertad, y ocurre incluso cuando la seguridad es fingida, o cuando las medidas son más restrictivas que libertadoras, porque la sensación de amparo que proporcionan, puede hacer que llegue a compensarnos soportarlas. SCHNEIER dice exactamente que: "Seguridad es un sentimiento y una realidad. La propensión para el teatro de seguridad viene de la interacción entre el público y sus líderes. Cuando la gente tiene miedo, es necesario que se haga algo que les haga sentirse seguros, aunque en realidad no hacen más seguro. Naturalmente, los políticos quieren hacer algo en respuesta a la crisis, incluso si ese algo no tiene ningún sentido. (...) Haríamos mucho mejor al aprovechar las fortalezas inherentes de nuestras democracias modernas y las ventajas naturales que tenemos a los terroristas: nuestra capacidad de adaptación y supervivencia, nuestra red internacional de leyes y su aplicación, y de las libertades y las libertades que hacen que nuestra sociedad tan envidiable".

En Estados Unidos, tras los atentados del 1 de septiembre de 2001 de Nueva York, la preocupación por ese escenario de seguridad se tornó obsesión, y en Europa se mostró igual entre algunos dirigentes. En general en aquel momento se proponían medidas de seguridad, tecnológicas, legales y procesales, que esencialmente iban dirigidas a la identificación de las personas y a legitimar la intrusión de las autoridades públicas en la vida privada, con el fin de vigilar cada movimiento en tiempo real. Por fortuna, diferentes iniciativas de las Instituciones encargadas de velar por los derechos humanos recordaron los pilares básicos del equilibrio para los debates entre los Estados Miembros.

---

[765] SCHNEIER B. *Beyond Security Theater*. 13 de Noviembre de 2009. Disponible en: http://www.schneier.com/blog/archives/2009/11/beyond_security.html

El Grupo de Trabajo del Artículo 29, siendo su presidente STEFANO RODOTÁ, emitió en el año 2001 un Dictamen relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo[766]. En él, se subrayaba concretamente "la necesidad de tener en cuenta la incidencia a largo plazo de políticas que se están aplicando rápidamente con carácter urgente o que se están proyectando en la actualidad. Esta reflexión a largo plazo es necesaria, máxime teniendo en cuenta que el terrorismo no es un fenómeno nuevo y que no se puede calificar de fenómeno temporal. El Grupo de Trabajo subraya también la obligación de respetar el principio de proporcionalidad en relación con toda medida de restricción del derecho fundamental del respeto a la vida privada".

La proporcionalidad es un principio indispensable, que debe observarse al establecer cualquier medida restrictiva de derechos en un Estado democrático. Todo Estado Miembro tiene la obligación "de demostrar que toda medida adoptada responde a una "exigencia social imperativa". Las medidas simplemente "útiles" o "convenientes" no pueden restringir los derechos y las libertades fundamentales", y en este sentido, el Grupo de Trabajo mostró su preocupación por el hecho de que materias como la protección de datos de carácter personal, se estuvieran exponiendo cada vez más como un obstáculo a la lucha eficaz contra el terrorismo. Reseñó que "las medidas contra el terrorismo no deben reducir los niveles de protección de los derechos fundamentales que caracterizan a las sociedades democráticas. Uno de los elementos clave de la lucha contra el terrorismo es la necesidad de preservar los valores fundamentales que constituyen el fundamento de nuestras sociedades democráticas y los valores que precisamente intentan destruir los que abogan por el recurso a la violencia".

En el equilibrio entre la libertad y la seguridad está la clave[767].

---

[766] Dictamen 10/2001 relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo, aprobado el 14 de diciembre de 2001. Grupo de Trabajo del Artículo 29 de la Directiva 95/66/CE.

[767] "El equilibrio entre protección de datos y seguridad ha de partir del reconocimiento del derecho de las sociedades democráticas a adoptar medidas que garanticen la seguridad pública, pero con pleno respeto a los derechos fundamentales, y en particular a los principios que configuran el contenido esencial del derecho a la protección de datos". "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio". Documentos de trabajo 147/2009. Laboratorio de Fundación Alternativas, Nº. 147. 2009. p.19.

El Tribunal Constitucional alemán, en la sentencia de fecha 27 de febrero de 2008, sobre el registro oculto "on line" de ordenadores y su conflicto con los derechos fundamentales, puso de nuevo sobre la mesa esa prudencia que debe presidir la toma de decisiones en materia de Seguridad de Estado. La excesiva ambición de seguridad puede afectar a los particulares en su desarrollo personal, tanto individualmente, como siendo parte de la comunidad, de una generalidad indeterminada, pero en ambos casos, "el principio de libertad ha de ser considerado como elemento objetivo esencial de todo ordenamiento democrático libre"[768]. Por ejemplo, en el caso de medidas de seguridad que impliquen la obtención de informaciones contenidas en sistemas informáticos, es esencial que esa información sea relevante para la protección y la seguridad estatal o para la protección de un bien jurídico de especial importancia, no bastando alegar otros intereses de menor relevancia, así como que un juez pueda supervisar la materialización de dichas medidas. En el año 2010, de nuevo el Tribunal Constitucional alemán[769], ha recordado que no todo vale en la persecución del terrorismo y la delincuencia organizada, y ante la denuncia de más de 35.000 ciudadanos, ha sentenciado que el almacenamiento masivo de comunicaciones electrónicas vulnera gravemente los derechos libertades de los ciudadanos, al prescindir del principio de proporcionalidad.

Ante la pregunta básica de si los ciudadanos deben ceder su libertad al Estado para obtener mayor seguridad, los Tribunales Constitucionales europeos están abogando en general por el respeto del equilibrio de intereses. Es obligación de los Estados garantizar la seguridad pública, pero el Estado de Derecho ha de guiar la toma de decisiones en esta materia. Y hay otras preguntas que pueden complicar esa duda: ¿se puede tener total seguridad siendo menos libres?, ¿se puede ser totalmente libre sin tener seguridad?, ¿cuánta libertad individual nos roba la seguridad?, ¿en qué

[768] LORENZ, D. "El registro oculto de ordenadores como desafío en la dogmática de los derechos fundamentales … Op.cit., p.13.

[769] La Ley de Acopio y Almacenamiento de Datos, aprobada en el año 2008, fue llevada ante el Tribunal Constitucional Federal en una demanda colectiva, frente a la cada vez mayor ligereza con la que el Estado se inmiscuye en la esfera privada. Pero el Tribunal no ilegalizó el almacenamiento masivo de correos electrónicos y conversaciones de móviles, la sentencia sólo declara anticonstitucional la manera en la que eso se hace, porque atenta contra el derecho al secreto de las telecomunicaciones. Los datos deben ser almacenados de forma diferenciada y separada, deben ser codificados, y deben ser susceptibles de ser tratados de una forma "transparente". BVerfG, 1 BvR 256/08 vom 2.3.2010. Disponible en alemán en: http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

casos, si los hay, puede o debe el Estado restringir las libertades?, ¿es posible el equilibrio entre libertad y seguridad?.

En el IX Congreso Nacional de la Abogacía[770] española se cuestionó la importancia de estos interrogantes, y diferentes expertos muy críticos con la ambición del control estatal ofrecieron interesantes opiniones. Entre las respuestas habidas destacan algunas como la de CHARLES CLARKE, ex ministro británico de Interior, que dijo que "en determinadas circunstancias, los ciudadanos aceptarán algunos sacrificios en su libertad, si se les asegura transparencia para entender el porqué"; la de ADELA CORTINA, Catedrática de Ética y Filosofía Política de la Universidad de Valencia, que condenó "el paternalismo político, según el cual, los gobernantes deciden en qué consiste el bien del pueblo"; la de ROBERT GOLDMAN, del Washington College of Law de la American University, que asegura que "el equilibrio entre libertad y seguridad es falso. Libertad y seguridad son dos conceptos complementarios"; la de KOFI ANAN, ex -secretario general de Naciones Unidas, que lamenta que "los expertos internacionales en derechos humanos, incluidos los del sistema de las Naciones Unidas, coinciden unánimemente en considerar que muchas de las medidas que adoptan actualmente los Estados para luchar contra el terrorismo, vulneran los derechos humanos y las libertades fundamentales"; la de JORGE DEZCALLAR, diplomático y ex – director del CNI, que explica que "todos queremos libertad con seguridad. Para conseguir mayor seguridad y libertad hay que reducir la amenaza terrorista y nuestra vulnerabilidad. Lo primero se consigue con medidas para combatir el terrorismo y sus causas; lo segundo, haciéndonos más fuertes ante la amenaza. Hay mucho margen para combatir el terrorismo dentro de la ley, con medidas bien definidas y sometidas al control judicial. Europa nunca ha sido más libre, más próspera y más segura que en la actualidad... gracias a valores compartidos como la libertad, la democracia, la solidaridad, el imperio de la ley y el respeto por los derechos humanos y las libertades individuales"; la de NICHOLAS HOWEN, que fue secretario general de la Comisión Internacional de Juristas, que señala que "el derecho y la legislación sobre derechos humanos son

[770] "¿Ceder libertad para lograr más seguridad?" Revista *Abogados*, nº 45. Madrid. Septiembre 2007. p.8.

armas fundamentales en la lucha contra el terrorismo y tiene la solidez suficiente para abordarla"; la de TERRY DAVIS, ex – secretario general del Consejo de Europa, que decía que "es posible conciliar seguridad y libertad si se descartan las medidas arbitrarias por parte de los Estados"; la de MANUEL CASTELLS, director del Internet Interdisciplinary Institute en la Universitat Oberta de Catalunya, que entiende que "la vulnerabilidad de los sistemas informáticos plantea una contradicción creciente entre seguridad y libertad en la red. Por un lado es obvio que el funcionamiento de la sociedad y sus instituciones y la privacidad de las personas no puede dejarse al albur de cualquier acción individual o de la intromisión de quienes tiene el poder burocrático o económico de llevarla a cabo. Por otro lado, como ocurre en la sociedad en general, con el pretexto de proteger la información en la red se renueva el viejo reflejo de control sobre la libre comunicación... De ahí que gobiernos y empresas busquen la seguridad mediante la regulación y la capacidad represiva de las instituciones más que a través de la autoprotección tecnológica de los ciudadanos. Es así como se reproduce en el mundo de Internet la vieja tensión entre seguridad y libertad"; la de GREGORIO PECES-BARBA, ex – rector de la Universidad Carlos III, que es consciente de la "difícil relación que actualmente se da entre libertad y seguridad, y como el miedo, la ignorancia o el ansia totalitaria de control de la ciudadanía están esforzándose para que el valor libertad aparezca como subsidiario del de seguridad ante cualquier amenaza"; y finalmente, la de EUGENIO TRÍAS, Catedrático de Historia de las Ideas en la Facultad de Humanidades de la Universidad Pompeu Fabra, que considera "respecto al valor seguridad debe decirse que encierra una paradoja en la que es importante insistir. Si se asume en exclusiva, o si se sitúa como "valor máximo" en el sentido nietzscheano, termina erosionando y aniquilando los demás valores (libertad, felicidad, igualdad, justicia)... La seguridad alberga la paradoja de que si se toma en exclusiva como máximo valor que orienta la praxis política acaba generando con harta frecuencia un escenario de infinita inseguridad, de manera que las medidas que se adoptan para atajarla son a veces las que acaban produciendo un máximo de aquello mismo que se quiere combatir. Es pésimo negocio existencial y político sustituir el miedo a nuestros semejantes, en el sentido de Hobbes, por a enajenación de nuestra libertad en un instrumento que termine diseminando

por todas partes algo a todas luces mucho más tenebroso que el miedo, el terror".

Todas estas opiniones son reflejo de que existe consciencia del peligro al que se exponen las libertades cuando la seguridad invade las parcelas de su ejercicio, sin embargo, sucede que en el momento de poner en práctica estos argumentos, se viene priorizando por defecto la protección del individuo como parte de la comunidad y, en general, las libertades pierde fuerza a favor de la utilidad económica o política que los Estados obtengan de cada medida.

La intimidad, el honor, la protección de datos personales, el secreto de las comunicaciones y la inviolabilidad del domicilio, son garantías que se consideran esenciales para que el individuo pueda desarrollarse como persona en la comunidad; le permiten decidir sobre su propio espacio individual, aislado del conocimiento de terceros. Por tanto, es evidente que una tutela efectiva de la privacidad es esencial para que una sociedad pueda seguir llamándose "democrática"[771]. La idea del "ciudadano de cristal" no puede aceptarse en un Estado de Derecho, pues refleja la idea de un Estado que puede adueñarse de la vida de sus ciudadanos, y eso es lo propio de los regímenes totalitarios, de "estados de policía" cuya principal preocupación es el control del individuo a pesar de que prometen un futuro lleno de eficiencia tecnológica.

Tradicionalmente se suspendía o limitaba el ejercicio de derechos fundamentales siempre a favor de la supervivencia de la comunidad y, en situaciones excepcionales, como una guerra. Hoy, esta "guerra" ha sido sustituida por el problema del terrorismo, un problema de naturaleza atemporal, ilimitada, respecto del anterior concepto. Y se pregunta el profesor RODOTÁ si también la limitación de derechos y garantías de ser infinita. Señala que, en todo caso, deberá responderse bajo criterios de "legitimidad" y "proporción entre medios y fines", y por supuesto, evitando identificar "seguridad" con "menos privacidad". Las medidas que requieran

[771] RODOTÀ, S. "Democracia y protección de datos". *Cuadernos de derecho público*, Nº 19-20. Madrid, 2003. pp. 15-26.

el tratamiento de datos personales, debe tenerse en cuenta que se ha de contar con habilitación legal suficiente, que se ha de respetar el derecho a la información y la transparencia de la actuación administrativa, que se limitará a determinadas y concretas finalidades, que los datos no podrán ser excesivos o no pertinentes en relación con esas finalidades (calidad del dato), que los sistemas informáticos que se utilicen para el tratamiento han de ser seguros, y que una autoridad independiente facilitará a los ciudadanos un canal de interlocución con el Estado, en todo lo que afecte al tratamiento de sus datos personales[772].

El control tecnológico indiscriminado y universal, en que la vigilancia pasa de tener un carácter excepcional a ser lo cotidiano, que pasa de establecerse para las "clases peligrosas", a preverse para la generalidad de las personas, acabará indefectiblemente derivando en el control del comportamiento, de sus decisiones y movimientos (por ejemplo, con tecnologías de RFID), pudiendo provocar una reconstrucción interesada de sus relaciones y costumbres.

La relación pacífica entre tecnología y democracia implica el reconocimiento del artículo 18.4 de la CE, cuyo papel es garantizar que no se pueda condicionar el comportamiento de las personas a través del control de cada aspecto de su vida. Esta garantía debe impedir que se pueda aislar e individualizar a los ciudadanos con precisión matemática en cada rasgo de su vida, para integrarlos después en una masa social teledirigida por el único camino que el Estado quiera ofrecer. Es precisamente obligación de los Estados impedir que un ataque terrorista pueda destruir el modo de vida de un país, impedir que la reacción de la comunidad ante este tipo de ataques provoque daños aún más devastadores, pues cuanto más convertimos nuestras fronteras y edificios en fortalezas, cuanto más se socavan nuestras leyes y más reducimos nuestras libertades, más dictatorial y menos democráticas serán nuestras vidas.

[772] "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio". *Documentos de trabajo 147/2009.* Laboratorio de Fundación Alternativas, Nº. 147. 2009. pp.29 y 30.

BIBLIOGRAFÍA

ABA CATOIRA, A. "El Estado de Alarma en España". *Teoría y Realidad Constitucional* nº 28. UNED. 2011. pp. 305-334. Disponible en: http://e-spacio.uned.es/fez/eserv.php?pid=bibliuned:TeoriayRealidadConstitucional-2011-28-2080&dsID=Documento.pdf

ACED FÉLEZ, E. Subdirector General de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid. Ponencia "Novedades del Reglamento de desarrollo de la LOPD". VI Jornada de Protección 2 de Datos Sanitarios. Madrid, 23 de abril de 2008.

ALBÁCAR LÓPEZ, J. L. *Protección de los derechos fundamentales en la nueva Constitución Española.* Texto de la ponencia española en la IV conferencia de Tribunales Constitucionales. Serie Discursos. Ed. Viena Panorama. Madrid, 1978.

ALONSO ALONSO, A. "Las bases de datos de ADN en el ámbito forense". Ed. Instituto Nacional de Toxicología y Ciencias Forenses. Departamento de Madrid. Centro de Estudios Jurídicos. Ministerio de Justicia. Madrid, 2003. www.cej.justicia.es/pdf/publicaciones/medicos_forenses/MEDI23.pdf

ALONSO GARCÍA, E. *La interpretación de la Constitución.* Ed. Centro de Estudios Constitucionales. Madrid, 1984.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J.M. *La defensa de la intimidad de los ciudadanos y la tecnología informática*. Ed. Aranzadi Editorial. Navarra, 1999.

ÁLVAREZ RIGAUDIAS, C. "El Nuevo reglamento de desarrollo de la LOPD" *Actualidad Jurídica* Nº 21. Uría Menéndez. 2008. pp. 25 – 33.

ARAGÓN REYES, M. "Intervenciones telefónicas y postales (Exámen de la jurisprudencia constitucional)". *Revista Teoría y Realidad Constitucional* nº 25. Ed. Centro de Estudios Ramón Areces. UNED. 2010.

BALAGUER CASTEJÓN, F. (Coord.) y CÁMARA VILLAR, G., LÓPEZ AGUILAR, J.F, CANO BUESO, J., BALAGUER CALLEJÓN, M.L. *Manual de Derecho Constitucional*. Vol.II. "Derechos y libertades fundamentales deberes constitucionales y principios rectores instituciones y órganos constitucionales". 6ª Ed. Tecnos. Madrid, 2011.

BAÓN RAMÍREZ, R. "Visión General de la Informática en el nuevo Código Penal". *Revista del Consejo General del Poder Judicial*, Núm. XI. Ámbito jurídico de las tecnologías de la información. Madrid, 1996.

BEJAR, H. *El ámbito de lo íntimo*. Ed. Alianza. Madrid, 1990.

BENTHAM, J. *Anarchical Fallacies*. Works Vol. 2. Ed. Bowring- Edinburgh, 1843. http://www.ditext.com/bentham/bentham.html

BLANC ALTEMIR, A. *La protección internacional de los derechos humanos a los cincuenta años de la Declaración Universal.* Ed. Tecnos. Madrid, 2001.

BOBBIO, N.

- "Presente y porvenir de los derechos humanos"*. Anuario de los Derechos Humanos*. Nº 2 (Enero). Madrid, 1982.
- *Teoría General del Derecho*. Ed. Debate. Madrid, 1991.

BRAGE CAMAZO, J. *Los límites a los derechos fundamentales*. Ed. Dykinson. 2004.

BRU PERAL, E.V. "Estados de alarma, excepción y sitio". *Derechos y Libertades. Revista del Instituto de Derechos Humanos Bartolomé de las Casas*, nº 7. Universidad Carlos III. Madrid, 1999. http://e-archivo.uc3m.es/dspace/bitstream/10016/1354/1/DyL-1999-IV-7-Bru.pdf

CARMONA Y CHOUSSAT, J.F. *Constituciones: interpretación histórica y sentimiento constitucional*. *Cuatro ensayos sobre organización política.* Ed. Thomson – Civitas. Navarra, 2004.

CARRILLO SALCEDO, J. A. *Soberanía de los Estados y derechos humanos en Derecho Internacional.* Ed. Tecnos. Madrid, 2001.

CARRILLO, M.

- *El derecho a no ser molestado. Información y vida privada.* Ed. Aranzadi. Navarra, 2003.
- "El juez ante las escuchas telefónicas". *El País.* 25 de marzo de 2010. http://elpais.com/diario/2010/03/25/opinion/1269471604_850215.html

CASAS BAAMONDE, Mª E. y RODRÍGUEZ – PIÑERO Y BRAVO – FERRER, M. (Directores). *Comentarios a la Constitucion Española. XXX Aniversario.* Fundación Wolters Kluwer. Madrid, 2009.

CASTÁN TOBEÑAS, J.

- *Poder Judicial e independencia judicial.* Ed. Reus. Madrid, 1951.
- *Los derechos del Hombre*. Ed. Tecnos. Madrid, 1968.

CASTRO BONILLA, A. "La protección del derecho a la intimidad en el tratamiento de datos personales: el caso de España y la nueva legislación latinoamericana". *Revista Digital Alfa-Redi*, nº 111. Diciembre - 2002. http://www.alfa-redi.org/revista/revista.asp?idRevista=55

CONSTANT, B. *De la libertad de los antiguos comparada con la de los modernos.* Escritos Políticos. Centro de Estudios Políticos y Constitucionales. Madrid, 1989.

COLLADO GARCÍA-LAJARA, E. *Protección de datos de carácter personal. Legislación, comentarios, concordancias y jurisprudencia*. Ed. Comares. Granada, 2000.

COTINO HUESO, L.

- y CAVANILLAS MÚGICA, S. *Libertades, democracia y gobierno electrónicos*. Colección Sociedad de la Información, nº 9. Ed. Comares. Granada, 2006.
- (coord.) *Democracia, participación y voto a través de las nuevas tecnologías*. Col. Sociedad de la Información nº 13. Ed. Comares. Granada, 2007.
- (coord.) *Libertad en internet. La red y las libertades de expresión e información*. Ed. Tirant lo Blanch. Valencia, 2007.
- y VALERO TORRIJOS, J. (coords.) *Administración electrónica. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*. Ed. Tirant lo Blanch. 2010.
- (editor) *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*. Publicaciones de la Universidad de Valencia. Valencia, 2011.

CHRISTIAN HESS, A. "Derecho a la intimidad y autodeterminación informativa". Artículo publicado en la R*evista electrónica del proyecto Democracia Digital.* Enero - 2002. http://www.democraciadigital.org.

CRUZ VILLALÓN, P.

- *El estado de sitio y la Constitución.* Centro de Estudios Constitucionales. Madrid, 1980.
- *Estados excepcionales y suspensión de garantías*. Ed. Tecnos. Madrid, 1991.
- "Los derechos al honor y a la intimidad como límite a la libertad de expresión, en la doctrina del Tribunal Constitucional". En *Cuadernos de derecho judicial*, CGPJ. Nº 12. Madrid, 1993.
- *La Constitución inédita: Estudios ante la constitucionalización de Europa*. Ed. Trotta. Madrid, 2004.

DANZIN, A. "Informática ¿técnica de opresión o de liberación?". *Nuestro Tiempo*, nº 262. Servicio de publicaciones de la Universidad de Navarra. 1976.

DAVARA RODRÍGUEZ, M.A.

- "La Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)". *Quince años de encuentros sobre informática y derecho* (1987 – 2002). Tomo I. Universidad Pontificia de Comillas (ICADE). Madrid, 2002. pp. 157 – 173.
- *Manual de Derecho Informático* (10ª edición). Ed. Aranzadi. 2008.

DE ASÍS ROIG, R. *Valores, derechos y Estado a finales del S.XIX*. Edición y Prólogo de Eusebio Fernández García. Universidad Carlos III de Madrid. Ed. Dykinson. Madrid, 1996.

DE BARTOLOMÉ CENZCANO, J. C. *El orden público como límite al ejercicio de los derechos y libertades.* Centro de Estudios Políticos y Constitucionales. Madrid, 2002.

DEL PESO NAVARRO, E.

- y RAMOS GONZÁLEZ, M.A. *LORTAD. Reglamento de Seguridad.* Díaz de Santos. Madrid, 1999.
- *La Ley de Protección de datos: la nueva LORTAD.* Ed. Diaz de Santos. Madrid, 2000.
- "La seguridad de la información en la Ley de Protección de Datos de Carácter Personal". *XIII Encuentros sobre Informática y Derecho.1999 – 2000.* Universidad Pontificia de Comillas. Ed. Aranzadi. Madrid, 2000. p. 49.

DÍEZ-PICAZO Y PONCE DE LEÓN, L. "Genoma humano e identificación de la persona como problema jurídico", *El derecho ante el Proyecto Genoma Humano*, Vol. IV, Col. Documenta. Fundación BBVA. Bilbao, 1994.

DÍEZ-PICAZO GIMÉNEZ, L.Mª. *Sistema de derechos fundamentales*. Ed. Civitas. Madrid, 2003.

ENÉRIZ OLAECHEA, F.J. *La protección de los derechos fundamentales y las libertades públicas constitucionales en la Constitución Española*. Ed. Universidad Pública de Navarra, 2007.

ELVIRA PEALES, A. *Derecho al Secreto de las Comunicaciones*. Col Breviarios Jurídicos. Ed. Iustel. Madrid, 2007.

FAIRÉN GUILLÉN, V.

- *La identificación de personas desconocidas.* Ed. Civitas. Madrid, 1992.
- "El Habeas Data y su protección actual surgida en la Ley española de informática de Informática de 29 de octubre de 1992". En *Revista de Derecho Procesa*l. Ed. de Derecho Reunidas S.A. Madrid, 1996. pp. 523 - 527.

FERNÁNDEZ ENTRALGO, J. *Seguridad Ciudadana. Materiales de Reflexión. Crítica sobre la Ley Corcuera.* Ed. Trotta. Madrid, 1993.

FERNÁNDEZ HEVIA, J.M. *Acceso público a la documentación y protección de datos*. Dictamen del Supervisor Europeo de Protección de Datos. Documentos de Referencia, nº 1. Julio 2005. Boletín de la Asociación Asturiana de Bibliotecarios (AABADOM), nº XVI. Enero – Junio 2005. pp. 43 y 44. Disponible en: http://ria.asturias.es/RIA/bitstream/123456789/127/1/supervisor_proteccion dedatos.pdf

FERNÁNDEZ RODRÍGUEZ, J.J. *Secreto en intervención de las comunicaciones en Internet.* Estudios de Protección de Datos. Ed. Civitas. Madrid, 2004.

FERNÁNDEZ RODRÍGUEZ, TOMÁS R. (Coord.) *Lecturas sobre la Constitución española.* 2ª Ed. UNED. Facultad de Derecho. Madrid, 1979.

FERNÁNDEZ SEGADO, F.

- "La Ley Orgánica de los estados de alarma, excepción y sitio". *Revista de Derecho Político*, nº 11. UNED, 1981.
- "La obsolescencia de la bipolaridad "modelo americano – modelo europeo – Kelsiano" como criterio analítico del control de constitucionalidad y la búsqueda de una nueva tipología explicativa. Parlamento y Constitución". *Anuario de las Cortes Castilla la Mancha*, Nº 6, 2002.

FERRAJOLI, L. *Los Fundamentos de los Derechos Fundamentales*. Ed. Trotta. Madrid, 2001.

GARCÍA BEATO, M.J. "Principios y derechos en la Ley Orgánica 5/1992, de 29 de Octubre, y en la Directiva 95/46/CE". Jornadas sobre el derecho española a la protección de datos. Ed. Agencia de Protección de Datos española. 28, 29 y 30 de Octubre de 1996. pp. 33 – 55.

GARCÍA CUADRADO, A. *Derecho, Estado y Constitución. El Estatuto científico y otros temas fundamentales de derecho constitucional.* Ed. Club Universitario. Alicante, 2010.

GARCÍA DE ENTERRÍA, E.

- *La Constitución como norma y el Tribunal Constitucional*. Ed. Civitas, Madrid, 1985.
- *La Constitución juzgada por los juristas*. Estudios sobre la Constitución Española. Monografías, nº 7. Instituto de Derechos Humanos Bartolomé de las Casas. Universidad Carlos III. Madrid, 1994.
- *Curso de derecho administrativo. Vol. I y II*. 14ª Ed. Civitas. Madrid, 2008.
- *Democracia, Jueces y Control de la Administración.* Ed. Civitas. Madrid, 2009.

GARRIDO FALLA, F. (y otros). *Comentarios a la Constitución*. Ed. Civitas. Madrid, 2001.

GARRIGA DOMÍNGUEZ, A.

- "La nueva Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos personales". *Anales de la Cátedra Francisco Suarez nº 34. 2000.*
- *La protección de los datos personales en el Derecho español.* Universidad Carlos III de Madrid. Ed. Dykinson. Madrid, 1999.
- "Una nueva exigencia de la libertad: la protección de los datos sensibles". *Dereito-Revista Xurídica da Universidade de Santiago de Compostela*. Vol. 9. Nº 2. 2000.
- *Tratamiento de datos personales y derechos fundamentales*. Ed. Dikynson. Madrid, 2009.

GIMENO SENDRA, V.

- *El proceso de habeas corpus*. Ed.Tecnos. Madrid, 1985.
- "La intervención de las comunicaciones". *Diario La Ley nº 7192*, de 9 de Junio de 2009.

GOIG MARTÍNEZ, J.M. "La defensa política de la Constitución. Constitución y estados excepcionales (I)". *Revista de Derecho*, nº 4. UNED, 2009. pp.263 – 296.

GONZÁLEZ MURUA, A. R.

- "Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de datos", en *Revista Vasca de Administración Pública*, nº 37. 1993. pp. 227-270; y en *Informática y derecho: Revista iberoamericana de derecho informático*, nº 6-7. Madrid, 1994. pp. 203 - 248. http://www.uned.es/ca-merida/Dereinfor.htm
- "Algunas Reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales". *Informática y Derecho*, nº 6-7. UNED. Mérida, 1994. pp. 227-270.

GONZALEZ QUINZA, A. "El "caso Olaverri" recurso de amparo sobre el acceso a ficheros públicos automatizados de carácter personal". *Revista Actualidad Informática*, nº 10 (Enero). Ed. Aranzadi. Pamplona, 1994.

GONZÁLEZ URDÍNGUIO, A. y GONZÁLEZ GUTIERREZ DE LEÓN, Mª A. "La videovigilancia en el sistema democrático español: Análisis y crítica de la Ley Orgánica 4/1997, de 4 de Agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos", *Revista de la Facultad de Derecho de la Universidad Complutense*, nº 89. pp. 105-124.

GUDE FERNÁNDEZ, A. *El Habeas Corpus en España*. Ed. Tirant Lo Blanch. Madrid, 2008.

GUERRRERO PICÓ, Mª C.

- *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal.* Ed. Aranzadi, S.A, Navarra, 2006.
- "Operadores privados y seguridad pública: la retención de los datos a la luz de la sentencia PNR". *Revista Española de Protección de Datos*, nº 2. Ed. Thomson-Civitas. 2007. pp. 185-215.

GUILLÉN VÁZQUEZ, M. "Bases de datos de ADN con fines de investigación penal. Especial referencia al derecho comparado." Centro de Estudios Jurídicos. Ministerio de Justicia. Madrid, 2003. www.cej.justicia.es/pdf/publicaciones/fiscales/FISCAL40.pdf

HÄBERLE, P. (Brage Camazano, Joaquín, tr.) *La garantía del contenido esencial de los derechos fundamentales*. Ed. Dykinson. Madrid, 2003.

HASBROUCK, E. "Total Travel Information Awareness", disponible en la página web del Gobierno de EEUU, Transportation Security Administration (TSA) http://www.Hasbrouck.org/articles/travelprivacy.html

MEAD, G.H. *La Génesis del Self y el control social*. Traducido por Ignacio Sánchez de la Yncera, disponible en: http://dialnet.unirioja.es/servlet/fichero_articulo?codigo=758619&orden=81076

HEREDERO HIGUERAS, M.

- "La informática y el uso de la información personal". *Ribero y Santodomingo: Introducción a la informática jurídica*. Ed. Fundesco. Madrid, 1986.
- *La Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*. Ed. Tecnos. Madrid, 1996.
- *La Directiva Comunitaria de Protección de Datos de Carácter Personal. Comentario a la Directiva del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Ed. Aranzadi. Pamplona, 1997.

HESSE, K.

- *Escritos de Derecho Constitucional*. Traducción de Pedro Cruz Villalón (2ª Ed.). Centro de Estudios Constitucionales. Madrid, 1992.
- *Constitución y derecho constitucional*. Manual de derecho constitucional, BENDA E. 2ª Ed. Marcial Pons. Madrid-Barcelona, 2001.

HOBBES, T. *Leviatán*. Ed. Alianza. Madrid, 1999.

IGLESIAS-REDONDO, J. "En torno a la libertas". *Estudios en homenaje al profesor Juan Iglesias*. UCM. T. III. Madrid, 1988.

JELLINEK, G. *Teoría general del Estado.* Col. "Política y Derecho". Ed. Fondo de Cultura Económica. México, 2000.

JIMÉNEZ CAMPO, J.

- "La garantía *constitucional* del derecho al secreto de las comunicaciones", *Revista Española de Derecho Constitucional - Año 7,* nº 20. Madrid, 1987. pp. 35-82.
- *Derechos fundamentales, concepto y garantías*. Ed. Trota. Madrid, 1999.

JIMÉNEZ ESCOBAR, R. Informática y derecho a la intimidad: una concepción que debe arrumbarse". Jornadas de abogacía e Informática. Ilustre Colegio de Abogados de Barcelona. 1993. p.85. (En GONZÁLEZ MURÚA, A. R., "Comentario a la STC 254/1993, algunas consideraciones en torno al artículo 18.4 CE y la protección de los Datos Personales", en *Informática y derecho: Revista iberoamericana de derecho informático*, nº 6-7. 1994, Madrid. pp. 203-248. http://www.uned.es/ca-merida/Dereinfor.htm)

LAFUENTE BALLE, J.M. "Los estados de alarma, excepción y sitio". *Revista de derecho político*, nº 30. Madrid, 1989. pp. 23-54.

LASSALLE, J.M. *Locke, liberalismo y propiedad*. Servicio de Estudios del Colegio de Registradores. Madrid, 2003.

LESMES SERRANO, C. *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia.* Ed. Lex Nova. Valladolid, 2008.

LOCKE, J. *Ensayos sobre el gobierno civil (1660–1662).* Trad. Armando Lázaro. Ed. Aguilar, México, 1983.

LÓPEZ DIAZ, E. *El Derecho al Honor y el Derecho a la Intimidad: Jurisprudencia y Doctrina.* Ed. Dykinson. Madrid, 1996.

LÓPEZ GARRIDO, D. (Ed.) *Ley Orgánica de los estados de alarma, excepción y sitio*. *Serie I. Trabajos Parlamentarios* nº 11. Cortes Generales. Secretaría General (Dirección de Estudios). Madrid, 1984.

LÓPEZ LOMA, L. "El registro oculto "on line" y su conflicto con los derechos fundamentales según la doctrina alemana tras la sentencia del Tribunal Constitucional Federal del 27 de febrero de 2008". *Revista Española de Protección de datos*, nº 5. Ed. Thomson-Civitas. 2008. pp. 223-230.

LÓPEZ PINA, A. (ed.) *La garantía constitucional de los derechos fundamentales. Alemania, España, Francia e Italia.* Ed. Cívitas, Madrid, 1991.

LORENZ, D. "El registro oculto de ordenadores como desafío en la dogmática de los derechos fundamentales y la reciente respuesta por la Constitución alemana". *Revista Española de Protección de Datos*, nº 5. Ed. Thomson-Civitas. 2008. pp. 9 -24.

LOSANO, M. "El Proyecto de Ley sobre tutela de la persona respecto a la elaboración informática de los datos personales y disposiciones sobre el tema de ilícitos informáticos", *Quince años de encuentros sobre Informática y Derecho* (1987-2002), Tomo. I. Universidad Pontificia de Comillas (ICADE), Madrid, 2002. pp. 173 – 181.

LOSANO, M. G., PERÉZ LUÑO, P. y GUERRERO MATEUS, M. F. *Libertad informática y Leyes de protección de datos personales*. Centro de Estudios Constitucionales. Madrid, 1989.

LUCAS MURILLO DE LA CUEVA, P.

- *Derecho a la autodeterminación informativa*. Ed. Tecnos. Madrid, 1990.
- *Informática y Protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal).* Cuadernos y Debates nº 43. Centro de Estudios Constitucionales. Madrid, 1993.
- La construcción del derecho a la autodeterminación informativa. Jornadas sobre Tecnologías de la Información para la modernización de las Administraciones Públicas (TECNIMAP). Organizadas por el Ministerio de Administraciones Públicas en Salamanca. 1998. http://www.csi.map.es/csi/tecnimap/tecnimap1998/sp14.htm#5
- "La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos* nº 104. 1999.
- Ponencia *Avances Tecnológicos y Derechos Fundamentales*. Los riesgos del Progreso. Derechos Humanos y Nuevas Tecnologías. XIV Curso de Verano UPV. Col. "Jornadas sobre Derechos Humanos" nº 6. San Sebastián. 2002.
- "La primera jurisprudencia sobre el derecho a la autodeterminación informativa". *Datospersonales.org. Revista de la Agencia de Protección*

de Datos de la Comunidad de Madrid nº 1. Marzo - 2003. www.datospersonales.org

- "Los derechos fundamentales al secreto de las comunicaciones y a la autodeterminación informativa". *Manuales de formación continuada*, nº 22 (Derechos procesales fundamentales). Ed. CGPJ. MFC. 2004. pp. 127-212.
- "Diez preguntas sobre el derecho a la autodeterminación informativa y la protección de datos de carácter personal". Conferencia que tuvo lugar el día 24 de octubre de 2005 en la sede de la Agencia Catalana de Protección de Datos: http://www.apd.cat/media/305.pdf
- y PIÑAR MAÑAS, J.L. *Derecho a la autodeterminación informativa.* Fundación Coloquio Jurídico Europeo. Madrid, 2009.
- "Novedades sobre el derecho a la protección de datos personales". Fundación Ciudadanía y valores. Curso de Verano: Organismos Internacionales y nuevo orden mundial. Aranjuez, 2010. http://www.funciva.org/uploads/ficheros_documentos/1284377010_pablo_lucas.pdf

MANNY, C. "La intimidad de la Unión Europea y la Seguridad de los Estados Unidos: la tensión entre la ley europea de protección de datos y los esfuerzos por parte de los Estados Unidos por utilizar los datos sobre pasajeros aéreos para luchar contra el terrorismo y otros delitos". *Cuadernos de Derecho Público* nº 19-20. 2003. (Ejemplar dedicado a: Protección de datos). pp. 145-178.

MARKOFF, J. "La vigilancia electrónica pone en peligro las libertades civiles". *El País*, 9 de Marzo de 2006. http://www.elpais.com/solotexto/articulo.html?xref=20060309elpepunet_5&type=Tes&k=vigilancia_electronica_pone_peligro_libertades_civiles#noticias

MARTÍN MORALES, R. *El régimen constitucional del secreto de las comunicaciones*. Ed. Civitas. Madrid, 1995.

MARTÍN RETORTILLO, S. *La doctrina del ordenamiento jurídico de Santi Romano y algunas de sus aplicaciones en el campo del Derecho administrativo. (Estudio preliminar a la traducción de la obra de SANTI ROMANO, El ordenamiento jurídico).* Instituto de Estudios Políticos. Madrid, 1963.

MARTÍN-CASALLO LÒPEZ, J.J. "La Directiva 95/46/CE y su incidencia en el ordenamiento jurídico español". *Jornadas sobre el derecho español de la protección de datos*. Agencia de Protección de Datos. 28, 29 y 30 de Octubre de 1996. Madrid. pp. 11 - 31.

MARTÍN Y PÉREZ DE NANCLARES, J. "Órdago del tribunal Constitucional Alemán al proceso de integración europea (algo más que una sentencia crítica con el tratado de Lisboa)". *REAF* nº 13. Abril de 2011. pp. 97-145. http://www10.gencat.cat/drep/binaris/_reaf13_Martin_tcm112-152630.pdf

MARTÍN PALLÍN, J.A. "Constitucionalidad del número identificador único". *Jornadas sobre el derecho español de la protección de datos*. Agencia de Protección de Datos. 28, 29 y 30 de Octubre de 1996. Madrid. pp. 56 - 90.

MARTÍNEZ ESCRIBANO, A. Los derechos fundamentales y las nuevas tecnologías en el trabajo. *Revista Deliberación*, de la Asociación Profesional de la Magistratura nº 3. Junio - 2002. http://www.apmagistratura.com/apm/deliberacion/admjus01.htm

MARTÍNEZ DE PISÓN CAVERO, J. *El derecho a la intimidad en la jurisprudencia constitucional*. Ed. Civitas. Madrid, 1993.

MARTÍNEZ MARTÍNEZ, R.

- *Tecnologías de la Información, Policía y Constitución*. Ed. Tirant lo Blanch. Valencia, 2001.
- *Una aproximación crítica a la autodeterminación informativa*. Ed. Civitas. Madrid, 2005.
- Ficheros Policiales y Constitución. *Revista Datos Personales de la APDCM* nº 16. Julio - 2005. www.datospersonales.org

- "El Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de datos de Carácter Personal. Consideraciones Generales". *Revista española de Protección de Datos*. Ed. Thomson-Civitas. Madrid, 2007. pp. 41 – 63.

MATEU DE ROS CEREZO, R. "Estados de alarma, excepción y sitio". *Gobierno y administración en la Constitución.* Dirección General del Servicio Jurídico del Estado, Vol. 1. Madrid, 1988. pp. 165-205.

MOORE, G.E. "Progress in digital integrated electronics", *IEEE International Electron Devices Meeting*, Vol. 21. IEDM Technical Digest. 1975. http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=9941

MONTAÑÉS PARDO, M.A. *La intervención de las comunicaciones. Doctrina jurisprudencial*. Col. Cuadernos de Aranzadi Constitucional. Ed. Aranzadi. Pamplona, 1999.

MORALES PRATS, F.

- *La tutela penal de la intimidad: privacy e informática*. Ed. Destino. Madrid, 1984.
- "Riesgos para la intimidad". En Internet y Derecho Penal. *Cuadernos de Derecho Judicial*. Escuela Judicial. Consejo General del Poder Judicial. Madrid, 2001. pp. 65 – 81.
- "Protección penal de la intimidad, frente al uso ilícito de la informática en el Código Penal de 1995". En Delitos contra la libertad y Seguridad. *Cuadernos de Derecho Judicial*. Escuela Judicial. Consejo General del Poder Judicial. Madrid, 1996.
- "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio". *Comentarios a la parte Especial del Derecho Penal*. Ed. Aranzadi S.A. Pamplona, 1996.

MORENO CATENA, V., "Garantía de los derechos fundamentales en la investigación penal". En la Revista *Poder judicial*, bajo el título *Justicia Penal*. Número especial II. Ed. Consejo General Poder Judicial. Madrid, 1987. pp. 131 – 172.

NAVAS CASTILLO, A. "Los estados excepcionales y su posible control por el Tribunal Constitucional". *Revista de la Facultad de Derecho de la Universidad Complutense*, nº 87. UCM. 1997. pp. 133-164.

NARVÁEZ RODRÍGUEZ, A. *Intervenciones telefónicas: comentarios a la STC 49/1999, de 5 de abril*. Repertorio Aranzadi del Tribunal Constitucional. T II. Madrid, 1999. pp. 1757 - 1781.

OLMO FERNÁNDEZ-DELGADO, L. *El descubrimiento y revelación de secretos documentales y de las telecomunicaciones Estudio de artículo 197.1º del Código Penal*. Ed. Dykinson. Madrid, 2009.

ORTÍ VALLEJO, A. *El derecho a la intimidad e informática.* Ed. Comares. Granada, 1994.

OROZCO PARDO, G. "Los derechos de las personas en la LORTAD"*.* *Informática y Derecho*, nº 6-7. UNED. Mérida, 1994. pp. 151-202.

OTTO Y PARDO DE, **I.**

- *Derecho Constitucional. Sistema de fuentes*. Ed. Ariel. Barcelona, 1987.
- y Martin-Retortillo, L. *La regulación del ejercicio de los derechos y libertades. La garantía de su contenido esencial en el artículo 53.1 de la Constitución*. Derechos fundamentales y Constitución. Ed. Civitas. Madrid, 1988.

PALOMAR OLMEDA, A. "Los derechos personales en el ámbito de la protección de datos". *Revista española de Protección de Datos*. Ed. Thomson-Civitas. Madrid, 2007. pp. 9 – 41.

PECES–BARBA, G.

- *Derechos Fundamentales*. Ed. Latina Universitaria. Madrid, 1980.

- *La elaboración de la Constitución de 1978.* Centro de Estudios Constitucionales. Madrid, 1988.
- *Curso de derechos fundamentales*. BOE/Universidad Carlos III. Madrid, 1993.

PÉREZ LUÑO, A.

- "La protección de la intimidad frente a la informática en la Constitución española de 1978". *Revista de estudios políticos* nº 9. Madrid, 1979. pp. 59-72.
- "Informática y libertad: Comentario al artículo 18.4 de la Constitución". *Revista de estudios políticos* nº 24. Madrid, 1981. pp. 31-54.
- *Derechos Humanos, Estado de Derecho y Constitución*. Ed. Tecnos. Madrid, 1984.
- "Comentario legislativo: la LORTAD y los derechos fundamentales", *Derecho y Libertades. Revista del Instituto Bartolomé de las Casas, 1993.*
- "Dilemas actuales de la protección de la intimidad". Editor J. Mª Sauca. *Problemas actuales de los derechos fundamentales*. Universidad Carlos III. Madrid, 1994.
- *Los derechos fundamentales* (6ª ed.), Col. Temas Clave de la Constitución Española. Madrid, 1995.
- *Derechos Humanos y Constitucionalismo ante el Tercer Milenio*. Ed. Marcial Pons. Madrid, 1996.
- Estado constitucional y derechos de la tercera generación. *Anuario de Filosofía del Derecho*. Vol. XIV. Valencia, 1997.
- *La libertad informática Libertad informática y leyes de protección de datos personales.* Ed. Centro de Estudios Políticos y Constitucionales. Madrid, 1999.
- "Sobre el arte legislativo de birbiloque. La LOPRODA y la tutela de la libertad informática en España". *Anuario de Filosofía del Derecho*, de la Sociedad Española de Filosofía Jurídica y Política. 2001.

PIÑAR MAÑAS, J.L.

- "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas". *Cuadernos de derecho público nº 19-20. 2003* (Ejemplar dedicado a Protección de Datos*).* pp. 45-90*.*
- "Introducción y Presentación. Introducción: la protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", *Repertorio de legislación y jurisprudencia sobre protección de datos.* APDCM- Thomson Cívitas. Madrid, 2004. pp. 21 a 98.
- "Reflexiones sobre el derecho fundamental a la protección de datos personales*". Actualidad jurídica Uría & Menéndez* nº 12. Madrid, 2005. pp. 7-17.
- "¿Existe la privacidad?". *Inauguración Curso Académico 2008-2009.* CEU Ediciones. Madrid, 2008.
- "El derecho fundamental a la protección de datos personales. Contenidos esencial y retos actuales. En torno al nuevo Reglamento de Protección de datos". Estudio Introductorio. *Legislación de Protección de Datos*. José Luis Piñar Mañas y Álvaro Canales Gil. Ed. Iustel. Madrid, 2008.
- "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio". *Documentos de trabajo 147/2009*. Laboratorio de Fundación Alternativas nº. 147. 2009.
- y MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*. Fundación Coloquio Europeo. Madrid, 2009.
- y CANALES GIL, A. *Legislación de protección de datos; estudio introductorio sobre el nuevo Reglamento.* 2ª Ed. Iustel. Madrid, 2011.

POLIN R. *Politica y filosofía en Thomas Hobbes*. Prensas Universitarias de Francia. Paris, 1953.

PROSSER, W.L. "Privacy". California Law Review. Nº 48. 1960. pp. 383 – 423.
http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf

REBOLLO DELGADO, L.

- *Derechos fundamentales y protección de datos*. Ed. Dykinson. Madrid, 2004.
- "El secreto de las comunicaciones: problemas actuales". *Revista de Derecho Político* nº 48-49. UNED. 2000. pp. 351 – 382.

RIBAGORDA GARNACHO, A. "Las medidas de seguridad en el borrador de nuevo Reglamento de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal". *Revista Española de Protección de Datos*, Nº 2. Ed. Thomson-Civitas. 2007. pp. 41-215.

RIVES SEVA, A. *La intervención de las comunicaciones en el proceso penal*. Ed. Bosch. Barcelona, 2010.

RODOTÀ, S.

- "Democracia y protección de datos". *Cuadernos de derecho público*, Nº 19-20. Madrid, 2003. pp. 15-26.
- *La vita e le regole. Tra diritto e non diritto.* Feltrinelli. Milán, 2006. Trad. *La vida y las reglas. Entre el derecho y el no derecho*. Ed. Trotta. Fundación Alfonso Martín Escudero. Madrid, 2010.
- "Tecnología y Derechos Fundamentales". *Datospersonales.org*. Revista De la Agencia Española de Protección de Datos de la Comunidad de Madrid nº 8. Madrid, 2004. http://datospersonales.org/
- "La conservación de los datos de tráfico en las comunicaciones electrónicas". En: Segundo Congreso sobre Internet, derecho y política: análisis y prospectiva (monográfico en línea). *Revista de Internet, Derecho y Política* nº 3. UOC. 2006. http://www.uoc.edu/idp/3/dt/esp/rodota.pdf

RODRÍGUEZ LAÍNZ, J.L.

- *Intervención judicial en los datos de tráfico de las comunicaciones.* Ed. Bosch. Barcelona, 2003.

- "Secreto de las comunicaciones en intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea". *Diario la Ley*, nº 7351. 2010.
- *Estudios Sobre el Secreto de Las Comunicaciones Perspectiva Doctrinal y Jurisprudencial.* Ed. La Ley. Madrid, 2011.
- "Hacia un nuevo entendimiento de la protección integral de los dispositivos privados de almacenamiento electrónico de datos relativos a las comunicaciones (Comentario a la STC 173/2011, de 7 de Noviembre)". Revista ICAM *Otrosí*, nº 9. Madrid, 2012. pp. 28 – 40.

RODRÍGUEZ RUÍZ, B. *El secreto de las comunicaciones: tecnología e intimidad.* Ed. McGraw-Hill. Madrid, 1997.

ROMEO CASABONA, C. M.

- *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la información*, prólogo de José Antonio Martín Pallín. Ed. Fundesco. Col. Impactos. Madrid, 1988.
- *Bases de datos de perfiles de ADN y criminalidad.* Ed. Comares. Granada, 2002.

RUBIO LLORENTE, F. *La Constitución como fuente del Derecho*. Col. La Constitución española y las fuentes del Derecho. Vol. I. Instituto de Estudios Fiscales. Madrid, 1979.

SAINZ MORENO, F.

- "Secreto e información en el Derecho público", *Estudios sobre la Constitución española (Homenaje al profesor García de Enterría*) III. Ed. Cívitas. Madrid, 1991. pp. 2863 y ss.
- (Ed.) *Constitución Española*; *Serie I. Trabajos Parlamentarios*. Cortes Generales. Servicio de Estudios y Publicaciones. Madrid, 1980.

SALDAÑA SOLERA, J. "Videovigilancia y Protección de Datos Personales". *Revista Ayuntamiento XXI*. Editorial Difusión Jurídica y Temas de Actualidad S.A. nº 20. 2006. pp. 27 – 38.

SALGADO SEGUÍN, V.A. Protección jurídica de los datos personales: Aproximación a la LORTAD, publicado en la página web de la Universidad de Alicante, en *Guías de Interés: Protección de Datos*. 1998. http://www.ua.es/oia/es/legisla/articulo.htm

SÁNCHEZ – ARCILLA BERNAL, J. "La obra legislativa de Alfonso X el sabio". Revista general de legislación y jurisprudencia III. Nº 1. Marzo, 2003.

SÁNCHEZ AGESTA, L. *Historia del constitucionalismo español (1808 - 1936).* 4ª Ed. Centro de Estudios Constitucionales. Madrid, 1984.

SÁNCHEZ BRAVO, A.A. "La Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal: diez consideraciones en torno a su contenido". *Revista de Estudios Políticos* nº 111. 2001.

SÁNCHEZ FERRIZ, R. "Algunas reflexiones sobre la efectividad de los derechos", *Revista de Derecho Político* nº 36. UNED. 1992.

SÁNCHEZ MORÓN, M. "El derecho de acceso a la información de medio ambiente". *Revista de Administración Pública* nº 137. 1995. http://www.cepc.es/rap/Publicaciones/Revistas/1/1995_137_031.PDF

SANTAMARÍA PASTOR, J. Luis Cosculluela Montaner, Avelino Blasco Esteve, Antonio Jiménez - Blanco Carrillo de Albornoz, entre otros. *Comentario sistemático a la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (Ley 30/1992, de 26 de Noviembre)*. Ed. Carperi Rústica. Madrid, 1993.

SCHMITT, C. *Teoría de la Constitución*. Alianza Editorial. Madrid, 1982.

SCHNEIER, B. Our Data, Ourselves (15 de Mayo de 2008). http://www.wired.com/politics/security/commentary/securitymatters/2008/05/securitymatters_0515

SUAREZ FERNÁNDEZ, L. *La pragmática de Alcalá en a Política de los Reyes Católicos*. En Anales de la Academia Matritense del Notariado. T. 43. Ed. Edersa. Madrid, 2006.

TORRES MURO, I. "Artículo 116 CE: Los estados excepcionales". En CASAS BAAMONDE, Mª E., y RODRÍGUEZ – PIÑERO Y BRAVO – FERRER, M. (Directores). *Comentarios a la Constitución Española*. XXX Aniversario. Fundación Wolters Kluwer. Madrid, 2009. Título Primero.

TRONCOSO REIGADA, A.

- "La contribución de las Agencias Autonómicas al derecho fundamental a la protección de datos". *XVII Encuentros sobre Informática y Derecho. 2002 – 2003.* Universidad Pontificia de Comillas. Ed. Aranzadi. Madrid, 2003. p. 23 - 47.
- La protección de datos personales: una reflexión crítica de la jurisprudencia constitucional. *Cuadernos de derecho público* nº 19-20*.* (Ejemplar dedicado a: Protección de datos*). 2003.* pp. 231 – 334.
- *Estudios sobre Administraciones Públicas y protección de datos personales*, I Encuentro entre Agencias Autonómicas de Protección de Datos Personales. Ed. APDCM. Distribución Cívitas Ediciones S.L. Madrid (2006).
- "Transparencia administrativa y protección de datos personales". *V Encuentro entre Agencias Autonómicas de Protección de Datos Personales*. 28 de octubre de 2008. Madrid. pp. 23 - 188.
- *La protección de datos personales: en busca del equilibrio*. Tratados. Ed. Tirant lo Blanch. Valencia, 2010.

URBANO CASTRILLO, E. *El derecho al secreto de las comunicaciones*. Col. Derechos fundamentales. Ed. La Ley. Madrid, 2011.

VARELA SUANZES - CARPEGNA, J. *Constituciones y Leyes Fundamentales.* Tomo I. Ed. Iustel. Madrid, 2012.

VIDAL GÓMEZ ALCALÁ, R. *La Ley como límite de los derechos fundamentales*. Ed. Porrúa. México, 1997.

VIDAL PRADO, C. y DELGADO RAMOS, D. "Algunas consideraciones sobre la declaración del estado de alarma y su prórroga". *Revista Española de Derecho Constitucional* nº 92. Año 31. 2011.

VILLAVERDE MENÉNDEZ, I.

- "Protección de datos personales, derecho a ser informado, y autodeterminación informativa del individuo. A propósito de la STC 254/1993". *Revista Española de Derecho Constitucional* nº 41. 1994.
- *Los derechos del público*. Ed. Tecnos. Madrid, 1995.
- "Concepto, contenido, objeto y límites de los derechos fundamentales", en *La Democracia constitucional. Estudios en homenaje al profesor Francisco Rubio Llorente*. Aragón/ Jiménez/ Solozábal (Coord.). Congreso de los Diputados, Tribunal Constitucional, Universidad Complutense de Madrid, Fundación Ortega y Gasset. Centro de estudios Políticos y Constitucionales. Vol I. Madrid, 2002.
- "Ciberconstitucionalismo. Las TIC y los espacios virtuales de los derechos fundamentales". *Revista Catalana de Derecho Público* nº 45. 2007.

WESTIN, A.F. *Privacy and Freedom*. Atheneum. New York, 1967.

ZAMBRANO GÓMEZ, E. "La regulación de los ficheros policiales en España y su tratamiento en la Convención de Prüm: la perspectiva de las autoridades nacionales de protección de datos". *Revista Constitucional de Derecho Europeo* nº 7. 2007. pp. 167-180. http://www.ugr.es/~redce/

DOCUMENTACIÓN

- **BOLETÍN DE JURISPRUDENCIA CONSTITUCIONAL, Nº 33, 1984. TEXTO DEL RECURSO DE INCONSTITUCIONALIDAD CONTRA LOS ARTÍCULOS DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL,** presentado por LÓPEZ GARRIDO, D.

- **COMUNICACIÓN SOBRE UNA INICIATIVA DE LA COMISIÓN PARA EL CONSEJO EUROPEO EXTRAORDINARIO DE LISBOA LOS DÍAS 23 Y 24 DE MARZO DE 2000. E-EUROPE: UNA SOCIEDAD DE LA INFORMACIÓN PARA TODOS.**

- **COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES UN ENFOQUE GLOBAL DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA UNIÓN EUROPEA.** Un enfoque global de la protección de los datos personales en la Unión Europea. Bruselas, 4.11.2010. COM (2010) 609.

- ***CONSTITUCIÓN ESPAÑOLA: TRABAJOS PARLAMENTARIOS*. CORTES GENERALES, SERVICIO DE ESTUDIOS Y PUBLICACIONES. MADRID, 1980.**

- **DIARIOS DE SESIONES DEL SENADO-COMISIÓN DE CONSTITUCIÓN,** trabajos preparatorios de la Constitución de 1978.

- **DICCIONARIO DE LA REAL ACADEMIA DE LA LENGUA ESPAÑOLA.**

- **DICTAMEN 5/2002 SOBRE LA DECLARACIÓN DE LOS COMISARIOS EUROPEOS RESPONSABLES DE PROTECCIÓN DE DATOS EN LA CONFERENCIA INTERNACIONAL CELEBRADA EN CARDIFF (9-11 DE SEPTIEMBRE DE 2002) SOBRE LA RETENCIÓN SISTEMÁTICA OBLIGATORIA DE DATOS SOBRE**

TRÁFICO DE TELECOMUNICACIONES, APROBADO POR EL GRUPO DE TRABAJO DEL ARTÍCULO 29 EL 11 DE OCTUBRE DE 2002.

- **DICTAMEN 6/2002 RELATIVO A LA TRANSMISIÓN DE LISTAS DE PASAJEROS Y OTROS DATOS DE COMPAÑÍAS AÉREAS A LOS ESTADOS UNIDOS, GRUPO DE TRABAJO DEL ARTÍCULO 29, 24 DE OCTUBRE DE 2002.**

- **DICTAMEN 2/2004 SOBRE EL CARÁCTER ADECUADO DE LA PROTECCIÓN DE LOS DATOS PERSONALES INCLUIDOS EN LOS REGISTROS DE NOMBRES DE LOS PASAJEROS (PASSENGER NAME RECORDS, PNR) QUE SE TRANSFIEREN AL SERVICIO DE ADUANAS Y PROTECCIÓN DE FRONTERAS DE ESTADOS UNIDOS (BUREAU OF CUSTOMS AND BORDER PROTECTION, CBP) ADOPTADO POR EL GRUPO DEL ARTÍCULO 29, EL 29 ENERO DE 2004.**

- **DICTAMEN 4/2004 RELATIVO AL TRATAMIENTO DE DATOS PERSONALES MEDIANTE VIGILANCIA POR VIDEOCÁMARA, GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS, DE 11 DE FEBRERO DE 2004.**

- **DICTAMEN 4/2005 SOBRE LA PROPUESTA DE DIRECTIVA SOBRE LA CONSERVACIÓN DE DATOS TRATADOS EN RELACIÓN CON LA PRESTACIÓN DE SERVICIOS PÚBLICOS DE COMUNICACIÓN ELECTRÓNICA Y POR LA QUE SE MODIFICA LA DIRECTIVA 2002/58/CE, ADOPTADO POR EL GRUPO DE TRABAJO DEL ARTÍCULO 29, EL 21 DE OCTUBRE DE 2005.**

- **DICTAMEN 2/2007 RELATIVO A LA INFORMACIÓN DE LOS PASAJEROS EN RELACIÓN CON LA TRANSFERENCIA DE DATOS PNR A LAS AUTORIDADES DE LOS ESTADOS UNIDOS. ADOPTADO POR EL GRUPO DE TRABAJO DEL ARTÍCULO 29, EL 15 DE FEBRERO DE 2007.**

- **DICTAMEN 7/2010 RELATIVO A LA COMUNICACIÓN DE LA COMISIÓN EUROPEA SOBRE EL ENFOQUE GLOBAL DE LAS TRANSFERENCIAS DE DATOS DE LOS REGISTROS DE NOMBRES DE LOS PASAJEROS (PNR) A TERCEROS PAÍSES, ADOPTADO POR EL GRUPO DE TRABAJO DEL ARTÍCULO 29, EL 12 DE NOVIEMBRE DE 2010.**

- **DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS RELATIVO A LA COMUNICACIÓN DE LA COMISIÓN SOBRE EL ENFOQUE GLOBAL DE LAS TRANSFERENCIAS DE DATOS DE REGISTRO DE PASAJEROS (PNR, EN INGLÉS) A TERCEROS PAÍSES, APROBADO EL 19 DE OCTUBRE DE 2010.**

- **DIRECTRICES SOBRE VIDEOVIGILANCIA DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (EDPS - 2009).**

- **DOCUMENTO DE TRABAJO RELATIVO AL TRATAMIENTO DE DATOS PERSONALES MEDIANTE VIGILANCIA POR VIDEOCÁMARA, GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS, DE 25 DE NOVIEMBRE DE 2002.**

- **DOCUMENTO DE TRABAJO SOBRE DATOS GENÉTICOS, ADOPTADO EL 17 DE MARZO DE 2004, POR EL GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES, CREADO EN VIRTUD DEL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 24 DE OCTUBRE DE 1995.**

- **INFORMES JURÍDICOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS SOBRE VIDEOVIGILANCIA. Nº 116/2008, Nº 148/2008, Nº 337/2008 Y Nº 286/2009.**

- **INFORME DE SITUACIÓN RELATIVO A LA APLICACIÓN DE LOS PRINCIPIOS DE LA CONVENCIÓN 108 A LA RECOGIDA Y AL PROCESO DE LOS DATOS BIOMÉTRICOS. COMITÉ CONSULTIVO DE LA CONVENCIÓN, CREADO POR EL ARTÍCULO 31 DE LA**

DIRECTIVA 95/46/CE, PARA LA PROTECCIÓN DE LAS PERSONAS RESPECTO AL PROCESO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL. ESTRASBURGO, FEBRERO DE 2005.

- **INFORME ELABORADO POR LA COMISARÍA GENERAL DE POLICÍA JUDICIAL DEL CUERPO NACIONAL DE POLICÍA, SOBRE EL SISTEMA OPERATIVO SITEL**, a solicitud de la Audiencia Provincial de Madrid, Sección 1, en oficio libre con número de Identificación único 7015609/2009, Rollo: 31/2009, de fecha 4 de Enero de 2011.

- **INFORME ELABORADO POR LA SUBDIRECCIÓN GENERAL DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD, DEPENDIENTE DE LA SECRETARÍA DE ESTADO DE SEGURIDAD, SOBRE EL SISTEMA OPERATIVO SITEL,** a solicitud de la Audiencia Provincial de Madrid, Sección 1, en oficio libre, con número de Identificación único 7015609/2009, Rollo: 31/2009, de fecha 4 de Enero de 2011.

- **"INFORME SOBRE LA INTIMIDAD Y CUESTIONES AFINES". COMISIÓN CALCUTT.** Cuadernos del Consejo General del Poder Judicial. Trad. de M.E. Sánchez Suárez, 1991.

- **MEMORIAS DE LA AEPD.**

- **RECOMENDACIÓN 3/97 SOBRE ANONIMATO EN INTERNET, ADOPTADA POR EL GRUPO DE TRABAJO DEL ARTÍCULO 29, EL 3 DE DICIEMBRE DE 1997.**

- **RECOMENDACIÓN 3/99 SOBRE LA CONSERVACIÓN DE LOS DATOS SOBRE TRÁFICO POR LOS PROVEEDORES DE SERVICIO INTERNET A EFECTOS DE CUMPLIMIENTO DE LA LEGISLACIÓN ADOPTADA POR EL GRUPO DE TRABAJO DEL ARTÍCULO 29, EL 7 DE SEPTIEMBRE DE 1999.**

RECURSOS EN INTERNET

***Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States*, 28 May 2004.** Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf

Anteproyecto de Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno. Disponible en: http://www.leydetransparencia.gob.es/anteproyecto/

Anteproyecto de la Ley Orgánica de Desarrollo de los Derechos Fundamentales Vinculados al Proceso Penal y Anteproyecto de Ley de Enjuiciamiento Criminal (22 de Julio de 2011). Disponible en: http://www.mjusticia.gob.es/cs/Satellite/es/1288775266264/MuestraInformacion.html

***Aviation and Transportation Security Act*.** Disponible en: http://www.tsa.gov/research/laws/law_regulation_rule_0010.shtm

Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 10 de mayo de 2005, Programa de La Haya: "Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia". [COM (2005) 184 final – Diario Oficial C 236 de 24.9.2005]. Disponible en: http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/l16002_es.htm

Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (2004/496/EC). Disponible en: http://www.statewatch.org/news/2004/mar/eu-us-pnr.pdf

Curso de Derechos Humanos publicado por el Instituto de Estudios Políticos para América Latina y África. Disponible en: http://www.iepala.es/curso_ddhh/ddhh33.htm

Decisión de la Comisión de 14 de mayo de 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (Bureau of Customs and Border Protection). Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0535:ES:HTML

Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf

Decisión 2006/729/PESC/JAI del Consejo, de 16 de octubre de 2006, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos - Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:298:0027:01:ES:HTML

Decisión 2007/551/PESC/JAI del Consejo, de 23 de julio de 2007 , relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007) - Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007). Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:01:ES:HTML

Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:ES:PDF

Declaración de los Derechos del Hombre y del Ciudadano de 1789. Disponible en: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/espagnol/es_ddhc.pdf

Declaración Universal de Derechos Humanos, aprobada por la Asamblea General de Naciones Unidas, en su Resolución 217 A (III), el 10 de diciembre de 1948 en París. Texto original disponible en: http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/043/88/IMG/NR004388.pdf?OpenElement

Declaraciones del IV Congreso de "Jueces para la Democracia", *Sobre el proyecto de Ley Orgánica sobre protección de la Seguridad Ciudadana*. Logroño, 1991. Disponible en: http://www.juecesdemocracia.es/congresos/vicongreso/declaraciones/Sobre%20el%20proyecto%20de%20Ley%20Org%A0nica%20sobre%20Portecci%A2n%20de%20la%20S%85.pdf

Dictamen conjunto sobre la propuesta de Decisión marco del Consejo relativa al uso del registro de nombres de los pasajeros («Passenger Name Record» - PNR) a efectos de la aplicación de la ley, presentado por la Comisión el 6 de noviembre de 2007. Adoptado el 5 de diciembre de 2007 por el Grupo de Trabajo previsto en el Artículo 29. Adoptado el 18 de diciembre de 2007 por el Grupo de Trabajo sobre Policía y Justicia. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145_es.pdf

Documentos de información de las Naciones Unidas. Los Derechos Humanos hoy día: Una Prioridad de las Naciones Unidas. Los derechos humanos en acción. http://www.un.org/spanish/hr/HRToday/action.htm

European Parliament Votes to Go to Court on EU-US PNR Deal. Disponible en: http://www.statewatch.org/news/2004/apr/13ep-vote-pnr-court.htm

***Enhanced Border Security and Visa Entry Reform Act of 2002. Pub. L. No. 107-173 (H.R. 3525) Section-by-Section Explanation*.** Disponible en: http://www.ofr.harvard.edu/additional_resources/Summary_of_Enhanced_Border_Security_Reform_Act_HR3525.pdf

Estatutos de creación de la asociación **Comisión de Libertades e Informática**. Disponible en: www.asociacioncli.org

European Commission/US Customs Talks on PNR Transmission, Brussels, 17/18 February Joint Statement.
Disponible en: http://www.statewatch.org/news/2003/feb/11usdata2.htm

Evaluación Programática Ambiental de US-VISIT sobre Cambios Potenciales a los Procesos Administrativos Inmigratorios y de Fronteras. 10 de abril de 2006. Disponible en:
http://www.dhs.gov/xlibrary/assets/usvisit/US-VISIT_PEA_Spanish.pdf

Fuero de los Españoles de 1945. Biblioteca Virtual de Miguel de Cervantes. Disponible en:
http://www.cervantesvirtual.com/obra-visor/fuero-de-los-espanoles-de-1945--0/pdf/

Guía de Videovigilancia. Agencia Española de Protección de Datos. 2009. Disponible en:
https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

Information Awareness Office at Defense Advanced Research Projects Agency (DARPA). Disponible en:
http://www.darpa.mil/
http://infowar.net/tia/www.darpa.mil/iao/index.htm

Informe de la Comisión al Consejo y al Parlamento Europeo. Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE). Disponible en:
http://cde.gestiondocumental.info/juridica/aue/MAY11/30135.pdf

INSTRUCCIÓN 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. B.O.E nº 296, de 12 de Diciembre de 2006, p. 43458. Disponible en:
https://www.agpd.es/portalweb/canalresponsable/videovigilancia/common/Instruccion_1_2006_videovigilancia.pdf

Instrumento de adhesión de 17 de enero de 1985, de España al Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos, adoptado en Nueva York por la Asamblea General de las Naciones Unidas, el 19 de diciembre de 1966. Disponible en: http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1985-5259

Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. Disponible en: http://www.boe.es/diario_boe/txt.php?id=BOE-A-1979-24010

PNR: Opinion of the Fundamental Rights Agency. 2008. Disponible en: http://www.statewatch.org/news/2008/oct/ep-pnr-opinion-fra.pdf

Propuesta de decisión marco del Consejo de 6 de noviembre de 2007 sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record - PNR) con fines represivos. Disponible en: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14584_es.htm

Propuesta de Directiva del Parlamento Europeo y del Consejo , relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:ES:PDF

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Disponible en: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf

Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes. 2009. Disponible en: http://www.statewatch.org/news/2009/apr/eu-pnr-council-5618-rev1-09.pdf

Resolución del Parlamento Europeo sobre la transmisión de datos personales por las compañías aéreas en los vuelos transatlánticos. P5_TA(2003)0097; B5-0187/2003. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:081E:0105:0107:ES:PDF

The Problem of Definition Privacy and Confidentiality. From the U.S. Congress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information (OTA-TCT-576), Washington, DC., September 1993. Publised for the Charles Sturt University. Australia.

•FRIED, C. Privacy, Yale Law Journal. Vol. 77, Connecticut, 1968.

•WESTIN, A. Privacy and Freedom, Atheneum, New York, 1967.

•PARENT, W. A. Recent Work on the Conception of Privacy, American Philosophical Quarterly , VOI. 20, 1983.

Disponible en: http://www.csu.edu.au/learning/ncgr/gpi/odyssey/privacy/ota_pc.html

Tratado por el que se establece una Constitución para Europa [DOUE 16 de Diciembre de 2004 (C310)]. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:310:0001:0002:ES:PDF